

625-EMD-004

## **EOSDIS Maintenance and Development Project**

# **Training Material for the EMD Project Volume 4: System Administration**

July 2004

Raytheon Company  
Upper Marlboro, Maryland

# **Training Material for the EMD Project Volume 4: System Administration**

**July 2004**

Prepared Under Contract NAS5-03098  
CDRL Item #23

## **RESPONSIBLE AUTHOR**

<u>Ralph E. Fuller /s/</u>	<u>7/12/2004</u>
Ralph E. Fuller	Date
EOSDIS Maintenance and Development Project	

## **RESPONSIBLE OFFICE**

<u>Mary S. Armstrong /s/</u>	<u>7/12/2004</u>
Mary Armstrong, Deputy Program Manager	Date
EOSDIS Maintenance and Development Project	

**Raytheon Company**  
Upper Marlboro, Maryland

This page intentionally left blank.

# Preface

---

This document is a formal contract deliverable. It requires Government review and approval within 45 business days. Changes to this document will be made by document change notice (DCN) or by complete revision.

Any questions should be addressed to:

Data Management Office  
The EMD Project Office  
Raytheon Company  
1616 McCormick Drive  
Upper Marlboro, Maryland 20774-5301

## Revision History

Document Number	Status/Issue	Publication Date	CCR Number
625-EMD-004	Original	July 2004	

This page intentionally left blank.

# Abstract

---

This is Volume 4 of a series of lessons containing the training material for the Earth Observing System Data and Information System (EOSDIS) Maintenance and Development (EMD) Project. This lesson provides a detailed description of the process required for performing system administration of ECS.

**Keywords:** training, instructional design, course objective, startup, shutdown, backup, restore, user administration, security, Release 7.

This page intentionally left blank.

# Contents

---

## Preface

## Abstract

## Contents

## Introduction

Identification .....	1
Scope .....	1
Purpose .....	1
Status and Schedule .....	1
Organization .....	1

## Related Documentation

Parent Documents .....	3
Applicable Documents .....	3
Information Documents .....	3
Information Documents Referenced .....	3
Information Documents Not Referenced .....	4

## System Administration

Lesson Overview .....	7
Lesson Objectives .....	7
Importance .....	9



## Secure Shell (SSH)

Secure Access to ECS DAACs .....	11
Setting Up SSH .....	11
Remote SSH Access .....	12
Changing Your Passphrase .....	14

## System Startup and Shutdown

Cold Startup By Subsystem .....	15
Warm Startup .....	17
Updating leapsec.dat and utcpole.dat files .....	18
Normal Shutdown .....	18
Emergency Shutdown .....	20
System Shutdown by Server .....	21

## Checking the Health and Status of the System

WhatsUp Gold .....	23
Launching WhatsUp Gold and Displaying the Network Map .....	23
Responding to Color Alerts and Obtaining Status of a Node .....	25
Configuring a Popup Menu for a Node or Multiple Nodes .....	27
Using Network Tools .....	30
Using WhatsUp Gold Logs .....	37
Whazzup??? .....	38
Host Status .....	40
Verify Mode .....	44
Performance Management .....	44
ECS Assistant and ECS Monitor .....	48

## Tape Operations

Networker Administrator Screen .....	55
Labeling Tapes .....	56

Indexing Tapes .....	59
----------------------	----

## **System Backups and Restores**

Incremental Backup .....	65
Full System Backup .....	68
Single or Multiple File Restore .....	70
Complete System Restore .....	74

## **User Administration**

Screening Personnel .....	79
Screening Criteria .....	79
Screening Procedures .....	79
Adding a New User .....	80
Deleting a User .....	80
Changing a User's Account Configuration .....	82
Changing User Access Privileges .....	82
Changing a User Password .....	83
Checking a File/Directory Access Privilege Status .....	83
Changing a File/Directory Access Privilege .....	84
Moving a User's Home Directory .....	87

## **Commercial Off-the-Shelf (COTS) Software Administration**

Installation .....	89
Log Files .....	89
COTS Configuration .....	89

## **Security**

Generating Security Reports .....	91
User Activity Data .....	91
User Audit Trail Information .....	92

## **Practical Exercises**

Introduction .....	93
Equipment and Materials .....	93
System Startup and Shutdown .....	93
Tape Operations, System Backup and Restore .....	93
User Administration .....	94
System Maintenance .....	95

## **Slide Presentation**

Slide Presentation Description .....	97
--------------------------------------	----

# Introduction

---

## Identification

Training Material Volume 4 is part of Contract Data Requirements List (CDRL) Item 23, which is a required deliverable under the Earth Observing System Data and Information System (EOSDIS) Maintenance and Development (EMD) Contract (NAS5-03098).

## Scope

Training Material Volume 4 describes the procedures by which the system administrator performs system administration activities. This lesson is designed to provide the operations staff with sufficient knowledge and information to satisfy all lesson objectives.

## Purpose

The purpose of this Student Guide is to provide a detailed course of instruction that forms the basis for understanding system administration. Lesson objectives are developed and will be used to guide the flow of instruction for this lesson. The lesson objectives will serve as the basis for verifying that all lesson topics are contained within this Student Guide and slide presentation material.

## Status and Schedule

This lesson module provides detailed information about training for the current baseline of the system. Revisions are submitted as needed.

## Organization

This document is organized as follows:

Introduction:	The Introduction presents the document identification, scope, purpose, and organization.
Related Documentation:	Related Documentation identifies parent, applicable and information documents associated with this document.
Student Guide:	The Student Guide identifies the core elements of this lesson. All Lesson Objectives and associated topics are included.
Slide Presentation:	Slide Presentation is reserved for all slides used by the instructor during the presentation of this lesson.

This page intentionally left blank.

# Related Documentation

---

## Parent Documents

The parent documents are the documents from which the EMD Training Material's scope and content are derived.

423-41-01	Goddard Space Flight Center, EOSDIS Core System (ECS) Statement of Work
423-46-03	EMD Task 101 Statement of Work For ECS SDPS Maintenance
423-46-02	Contract Data Requirements Document for EMD Task 101 ECS SDPS Maintenance

## Applicable Documents

The following documents are referenced within this EMD Training Material, or are directly applicable, or contain policies or other directive matters that are binding upon the content of this document:

420-05-03	Goddard Space Flight Center, Earth Observing System (EOS) Performance Assurance Requirements for the EOSDIS Core System (ECS)
423-41-02	Goddard Space Flight Center, Functional and Performance Requirements Specification for the Earth Observing System Data and Information System (EOSDIS) Core System (ECS) (ECS F&PRS)
423-46-01	Goddard Space Flight Center, Functional and Performance Requirements Specification for the Earth Observing System Data and Information System (EOSDIS) Core System (ECS) Science Data Processing System (EMD F&PRS)

## Information Documents

### Information Documents Referenced

The following documents are referenced herein and amplify or clarify the information presented in this document. These documents are not binding on the content of the EMD Training Material.

290-004	Goddard Space Flight Center, Internet Protocol Operational Network (IONet) Access Protection Policy and Requirements
335-EMD-	EMD COTS Deployment Plan
609-EMD-001	Release 7 Operations Tools Manual for the EMD Project

611-EMD-001	Mission Operation Procedures for the EMD Project
910-TDA-022	Custom Code Configuration Parameters for ECS
NPR 1620.1A	NASA Procedural Requirements: Security Procedural Requirements
NPR 2810.1	NASA Procedural Requirements: Security of Information Technology
OMB Circular A-130	Office of Management and Budget, Management of Federal Information Resources

### **Information Documents Not Referenced**

The following documents, although not referenced herein and/or not directly applicable, do amplify or clarify the information presented in this document. These documents are not binding on the content of the EMD Training Material.

305-EMD-001	Release 7 Segment/Design Specification for the EMD Project
311-EMD-001	Release 7 Data Management Subsystem (DMS) Database Design and Database Schema Specifications for the EMD Project
311-EMD-002	Release 7 INGEST (INS) Database Design and Schema Specifications for the EMD Project
311-EMD-003	Release 7 Planning and Data Processing Subsystem Database Design and Schema Specifications for the EMD Project
311-EMD-004	Release 7 Science Data Server Database Design and Schema Specifications for the EMD Project
311-EMD-005	Release 7 Storage Management and Data Distribution Subsystems Database Design and Database Schema Specifications for the EMD Project
311-EMD-006	Release 7 Subscription Server Database Design and Schema Specifications for the EMD Project
311-EMD-007	Release 7 Systems Management Subsystem Database Design and Schema Specifications for the EMD Project
311-EMD-008	Release 7 Registry Database Design and Schema Specifications for the EMD Project
311-EMD-009	Release 7 Product Distribution Subsystem (PDS) Database Design and Database Schema Specifications for the EMD Project
311-EMD-010	Release 7 NameServer Database Design and Schema Specifications for the EMD Project
311-EMD-011	Release 7 Order Manager Server Database Design and Schema Specifications for the EMD Project
311-EMD-012	Release 7 Spatial Subscription Server Database Design and Schema Specifications for the EMD Project

311-EMD-013	Release 7 Data Pool Database Design and Schema Specifications for the EMD Project
313-EMD-001	Release 7 ECS Internal Interface Control Document for the EMD Project
152-TP-001	ACRONYMS for the EOSDIS Core System (ECS) Project
152-TP-003	Glossary of Terms for the EOSDIS Core System (ECS) Project



This page intentionally left blank.

# System Administration

---

## Lesson Overview

This lesson will provide you with the tools needed to perform the various tasks required to administer Implementation of the Earth Observing System Data and Information System (EOSDIS) Core System (ECS) during maintenance and operations.

## Lesson Objectives

**Overall Objective** - The overall objective of this lesson is proficiency in the various tasks required to administer the ECS during maintenance and operations.

**Condition** - The student will be given a copy of 609-EMD-001, *Release 7 Operations Tools Manual for the EMD Project*, a copy of 611-EMD-001, *Mission Operation Procedures for the EMD Project* and a functioning system.

**Standard** - The student will use the Procedures Manual in accordance with prescribed methods and complete required procedures without error to accomplish all tasks required.

**Specific Objective 1** - The student will perform a Secure Shell login to ECS and establish a personal passphrase.

**Condition** - The student will be given a copy of 609-EMD-001, *Release 7 Operations Tools Manual for the EMD Project*, a copy of 611-EMD-001, *Mission Operation Procedures for the EMD Project* and a functioning system.

**Standard** - The student will perform without error the procedures required to login to ECS using Secure Shell and establish a personal passphrase.

**Specific Objective 2** - The student will manually shutdown and restart a single subsystem of the ECS without affecting other subsystems.

**Condition** - The student will be given a copy of 609-EMD-001, *Release 7 Operations Tools Manual for the EMD Project*, a copy of 611-EMD-001, *Mission Operation Procedures for the EMD Project* and a functioning system.

**Standard** - The student will perform without error the procedures required to effect an orderly shutdown and startup of one subsystem of the ECS without compromising or otherwise affecting the other component subsystems from the command line.

**Specific Objective 3** - The student will shutdown and restart a single subsystem of the ECS using ECS Assistant without affecting other subsystems.

**Condition** - The student will be given a copy of 609-EMD-001, *Release 7 Operations Tools Manual for the EMD Project*, a copy of 611-EMD-001, *Mission Operation Procedures for the EMD Project* and a functioning system.

**Standard** - The student will perform without error the procedures required to effect an orderly shutdown and startup of one subsystem of the ECS without compromising or otherwise affecting the other component subsystems using the ECS Assistant.

**Specific Objective 4** - The student will conduct system performance monitoring, to include using WhatsUp Gold to check the health and status of the network and accessing the EOSDIS Mission Support Network (EMSn) Web Page.

**Condition** - The student will be given a copy of 609-EMD-001, *Release 7 Operations Tools Manual for the EMD Project*, a copy of 611-EMD-001, *Mission Operation Procedures for the EMD Project* and a functioning system.

**Standard** - The student will use Whazzup and ECS Monitor in accordance with specified procedures and without error to check the status of system servers.

**Specific Objective 5** - The student will label and index a tape cartridge.

**Condition** - The student will be given a copy of 609-EMD-001, *Release 7 Operations Tools Manual for the EMD Project*, a copy of 611-EMD-001, *Mission Operation Procedures for the EMD Project* and a functioning system.

**Standard** - The student will perform without error the procedures required to label a tape and index a tape cartridge.

**Specific Objective 6** - The student will create an incremental tape backup.

**Condition** - The student will be given a copy of 609-EMD-001, *Release 7 Operations Tools Manual for the EMD Project*, a copy of 611-EMD-001, *Mission Operation Procedures for the EMD Project* and a functioning system.

**Standard** - The student will perform without error the procedures required to create an incremental tape backup of system files created or modified within the past six days.

**Specific Objective 7** - The student will create a tape backup of the entire ECS system.

**Condition** - The student will be given a copy of 609-EMD-001, *Release 7 Operations Tools Manual for the EMD Project*, a copy of 611-EMD-001, *Mission Operation Procedures for the EMD Project* and a functioning system.

**Standard** - The student will perform without error the procedures required to perform a complete tape backup of the ECS.

**Specific Objective 8** - The student will restore individual files or entire volumes of backup tapes to the ECS system.

**Condition** - The student will be given a copy of 609-EMD-001, *Release 7 Operations Tools Manual for the EMD Project*, a copy of 611-EMD-001, *Mission Operation Procedures for the EMD Project* and a functioning system.

**Standard** - The student will perform without error the procedures required to perform individual or complete file restorations.

**Specific Objective 9** - The student will review and modify system logs.

**Condition** - The student will be given a copy of 609-EMD-001, *Release 7 Operations Tools Manual for the EMD Project*, a copy of 611-EMD-001, *Mission Operation Procedures for the EMD Project* and a functioning system.

**Standard** - The student will perform without error the procedures required to perform system log maintenance.

**Specific Objective 10** - The student will create, modify, and delete user accounts on the ECS.

**Condition** - The student will be given a copy of 609-EMD-001, *Release 7 Operations Tools Manual for the EMD Project*, a copy of 611-EMD-001, *Mission Operation Procedures for the EMD Project* and a functioning system.

**Standard** - The student will perform without error the procedures required to add a new user account to the ECS, make modifications to a variety of account access parameters, and delete the account from the ECS.

**Specific Objective 11** - The student will check and modify access privileges on files and directories across the ECS.

**Condition** - The student will be given a copy of 609-EMD-001, *Release 7 Operations Tools Manual for the EMD Project*, a copy of 611-EMD-001, *Mission Operation Procedures for the EMD Project* and a functioning system.

**Standard** - The student will perform without error the procedures required to check file and directory access privileges and modify them to allow or deny access by various classes of users.

**Specific Objective 12** - The student will determine when security breaches occur and will remedy such breaches.

**Condition** - The student will be given a copy of 609-EMD-001, *Release 7 Operations Tools Manual for the EMD Project*, a copy of 611-EMD-001, *Mission Operation Procedures for the EMD Project* and a functioning system.

**Standard** - The student will perform without error the procedures required to identify when security breaches occur and to remedy such breaches.

## **Importance**

A System Administrator's goal is to keep the computer system usable by the users. A system running at peak efficiency does so because of the proper use of the tools provided for and used by the System Administrator. Intimate knowledge of how each tool works and which should be used in a particular situation is crucial to satisfying the ECS user community.

This page intentionally left blank.

# Secure Shell (SSH)

---

Secure Shell is an application that greatly improves network security. Secure Shell is the standard for remote logins, solving the problem of hackers stealing passwords. Secure Shell secures connections by encrypting passwords and other data. Once launched, it provides transparent, strong authentication and secure communications over any IP-based connection. The SSH Secure Shell application is virtually invisible during day-to-day use. It provides a provides an extensive library of features for securing and authenticating terminal connections, file transfers or almost any other type of connection might be created over an IP network. Secure Shell is to be used for communication among system platforms and among the DAACs.

## Secure Access to ECS DAACs

ECS has implemented a Local Area Network (LAN) at the DAACs that is more secure than most other LANs. From the Internet, it is not possible to directly connect with all hosts at a DAAC. There is a set of hosts that are dual-homed to a user LAN that is connected on one side to the Internet and to the DAAC production LAN on the other side. This will require an interactive user to first use SSH to access a dual homed host and then use ssh to access a production host. In order to minimize the impact on the user, a single login has been implemented.

## Setting Up SSH

SSH programs have client and server components much like other network programs. The user only needs to be concerned with the client configuration as the server side is set up by a systems administrator. The amount of effort that it takes to get SSH going depends on how many different home directories the user has. At Landover, for instance, there are separate directories for the EDF and the VATC.

Most users will start from the same host whether from an X terminal, a UNIX workstation or a PC. Prior to executing **ssh** commands, use **setenv DISPLAY <IP address>:0.0** at your local host. To ensure system security, do not use the **setenv DISPLAY** command on subsequent hosts accessed via **ssh**. The process is started by running the **sshsetup** script, which will enable **ssh** to other hosts from which one may use the same home directory. The only thing you need to do before executing the script is to pick a good passphrase of at least 10 characters. You can, and should, use spaces and multiple words with numbers and misspellings and special characters. Note that passwords are NOT echoed back to the screen.

## Initiating SSHSETUP

---

- 1 Login into your normal Unix workstation where your home directory resides.

- 2 Initiate Secure Shell setup by typing **/tools/bin/sshsetup** then press **Return/Enter**.
    - You will see an information statement:  
**Use a passphrase of at least 10 characters which should include numbers or special characters and MAY include spaces**
  - 3 At the prompt "New passphrase:" **enter your passphrase <enter>**.
  - 4 At the prompt "Retype new passphrase:" **re-enter your passphrase <enter>**.
    - You will then see:  
**Initializing random number generator...**  
**Generating p: Please wait while the program completes ...**  
**%**
    - This establishes the .ssh sub-directory in your <username>/home directory, creates the local ssh key, and creates the necessary files.
- 

## Remote SSH Access

If you need to access a host with a different home directory, you will need to run the **sshremote** script. This script sets up the destination host with the new set of keys and transfers the source (local) key to the destination and the destination key to the source. You must have an existing account on the remote host.

### Setting Up Remote Access SSH

---

- 1 Login into your normal Unix workstation where your home directory resides.
- 2 Initiate Secure Shell remote setup by typing **/tools/bin/sshremote** then press **Return/Enter**.
  - You will see the following prompt:  
**You have a local passphrase. Do you want to setup for:**
    - 1 VATC
    - 2 EDF
    - 3 MiniDAAC
    - 4 GSFC DAAC
    - 5 GSFC M and O
    - 6 EDC DAAC
    - 7 EDC M and O
    - 8 LaRC DAAC
    - 9 LaRC M and O
    - 10 NSIDC DAAC

## 11 NSIDC M and O

### 12 Exit from script

Select:

- 3 At the "Select" prompt, type in the corresponding number to the desired host then press **Return/Enter**.

- You will receive a prompt similar to the following for the VATC:

**Working...**

- 4 At the prompt "Enter passphrase for RSA key '<username>@<hostname>': Type in your **passphrase** then press **Return/Enter**.

- A prompt similar to the following will be displayed:

**Last login: Thu Jul 9 10:41:13 1998 from echuser.east.hit  
No mail.  
Sun Microsystems Inc. SunOS 5.5.1 Generic May 1996  
t1code1{username}1:**

- 5 At the prompt "Press <ctrl>a to run sshsetup and exit <enter> to logoff t1code1u", type **<ctrl>-a** to initiate the sshsetup script on the remote host.

- You will see an information statement:

**Use a passphrase of at least 10 characters which should include numbers  
or special characters and MAY include spaces**

- 6 At the prompt "New passphrase:" **enter your passphrase <enter>**.

- 7 At the prompt "Retype new passphrase:" **re-enter your passphrase <enter>**.

- You will then see:

**Initializing random number generator...  
Generating p: Please wait while the program completes ...  
%**

- 8 At the "<hostname>" prompt type **exit** then press **Return/Enter**.

- The following information will be displayed:

**Updating locally...  
Updating t1code1u.ecs.nasa.gov  
%**

- This establishes the ssh key at the remote host and exchanges key information with your local host.

**NOTE:** The ssh keys at remote sites can be different from the local host ssh key.

---



## Changing Your Passphrase

Another script has been developed to change your passphrase on the local host and then transfer the key to the other environments. The **ssh** keys for remote hosts will have to be changed separately. Use the following procedure to change your passphrase:

### Changing Your Passphrase

---

- 1 Login to your normal Unix workstation where your home directory resides.
    - Initiate passphrase change by typing **/tools/bin/sshchpass** then press **Return/Enter**.
    - You will see an information statement:  
  
**Use a passphrase of at least 10 characters which should include numbers or special characters and MAY include spaces**
  - 2 At the prompt "Old passphrase:" **enter your old passphrase <enter>**.
  - 3 At the prompt "New passphrase:" **enter your passphrase <enter>**.
  - 4 At the prompt "Retype new passphrase:" **re-enter your passphrase <enter>**.
    - You will then see an information prompt similar to the following:  
  
**ssh-keygen will now be executed. Please wait for the prompt to Return!**  
**/home/bpeters/.ssh/authorized\_keys permissions have already been set.**  
**%**
-

# System Startup and Shutdown

---

Starting or shutting down a computer system may involve nothing more than turning a power switch to the on or off position. However, the interdependency of the various servers may require the System Administrator to startup or shutdown the servers in a particular order. Depending on the situation, the entire computer system may be started or stopped (cold) or only selected servers may be started or stopped (warm). The next sections cover the procedures and details of cold and warm startups and shutdowns.

A complete system startup and shutdown should only need to occur approximately once in three or four months during the early stages of system implementation due to the inherent instability of new systems. After the system stabilizes, it is estimated that complete system startups and shutdowns will occur only about once a year. Partial shutdowns and restarts will be performed as needed due to maintenance concerns.

## Cold Startup By Subsystem

A cold startup is indicated when there are no subsystems currently running, e.g., when the system is to be turned on for the first time, following a system maintenance operation that requires all power to be turned off, or following a power failure. In most situations a cold startup is also indicated by the power switch being in the OFF position.

The Cold System Startup is done in sequential order by subsystem, as follows:

- x0css02
- DNS Master Server
- NIS Master
- CSS Server
- x0mss0x
- ClearCase Server
- x0ins01
- Interface Server
- x0mshxx
- Tivoli Server
- x0acs0x
- PDPS
- Other Servers

## Performing Cold Subsystem Startup

---

- 1 Determine which machines perform the following functions. Some may perform multiple functions:
    - Domain Name Server (DNS) Master
    - Name Information Server (NIS) Master
    - Mail Hub Server(s)
    - Automount Servers
    - ClearCase Server
    - Communication Subsystem (CSS)
    - Other License Servers
    - Sybase SQL Servers
    - Data Server Subsystem (DSS)
    - Planning & Data Processing System (PDPS)
    - Client Subsystem (CLS)
  - 2 Startup the DNS Master, the NIS Master, and the CSS server. Once that system has booted without error, proceed to Step 3.
  - 3 Power on the ClearCase server(s). Once the systems(s) have booted without error, proceed to Step 4.
  - 4 Power on the Interface server(s). Once the system(s) have booted without error, proceed to Step 5.
  - 5 Power on the MSS server(s). Once the system(s) have booted without error, proceed to Step 6.
  - 6 Power on the DSS server(s). Once the system(s) have booted without error, proceed to Step 7.
  - 7 Power on the Ingest server(s). Once the system(s) have booted without error, proceed to Step 8.
  - 8 Power on the PDPS server(s). Once the system(s) have booted without error, proceed to Step 9.
  - 9 Power on the Client and Data Management server(s).
-

## Warm Startup

A warm startup is indicated when there are some subsystems currently running while others have been shutdown either due to operator intervention or an external malfunction. The subsystems not actively running need to be started without interfering with the current active operations. In some instances, a warm startup may require some active subsystems to be shutdown and restarted so that their interaction and connectivity will be properly resumed.

### Performing Warm Subsystem Startup

---

1 Determine which machines perform the following functions:

- Domain Name Server (DNS) Master
- Name Information Server (NIS) Master
- Mail Hub Server(s)
- Automount Servers
- ClearCase Server
- Communication Subsystem (CSS)
- Other License Servers
- System Management Subsystem
- Sybase SQL Servers
- Data Server Subsystem (DSS)
- Planning & Data Processing System (PDPS)
- Client Subsystem (CLS)

2 Determine which machine is currently down.

3 Determine the interoperability dependencies among the machines.

4 Turn on machines in an order consistent with the dependencies.

**NOTE:** In addition to warm system startup/reboot sequences, ECS servers that use the Sybase SQL server may need to be bounced whenever the SQL server is bounced. At present, this is certainly the case for all STMGT servers. That is, if the Sybase SQL server is stopped and restarted for any reason, all STMGT servers need to be stopped and restarted once the Sybase SQL server has come back on-line.

---

## Updating leapsec.dat and utcpole.dat files

In addition to starting system servers there are essential tasks that System Administrators must perform on a regular basis.

In order to ensure proper operation of Product Generation Executives (PGEs), two files must be updated weekly with data transferred from the U.S. Naval Observatory. These files are **`${PGSHOME}/database/common/TD/leapsec.dat`** and **`${PGSHOME}/database/common/CSC/utcpole.dat`**. The update of these files is accomplished by executing **`leapsec_update.sh`** and **`utcpole_update.sh`** in the **`/tools/admin/exec`** directory with root privileges. It has not been determined yet if these tasks will be accomplished manually or via cron job scripting.

## Normal Shutdown

A normal shutdown occurs when the operator is required to turn off the power to the entire system or any of the component subsystems. Normal shutdowns are scheduled by the Resource Manager with prior approval by the DAAC management at a time that minimizes disruption to system users, usually during off-hours. No loss of data is anticipated from a normal shutdown. All subsystems are shutdown in a routine fashion.

The system shutdown procedure is performed by the System Administrator at the discretion of the Network Administrator, usually for the purpose of repair. The system shutdown is normally performed in reverse order of the system startup as previously described. Prior to a normal shutdown, the System Administrator sends broadcast messages to all Computer Operators on the system at Shutdown Minus 30 minutes, Shutdown Minus 15 minutes, and Shutdown Minus 1 minute. At the scheduled shutdown time, the System Administrator blocks all incoming requests from the gateway and allows active jobs to complete (unless it is anticipated that they will take longer than 10 minutes, in which case the System Administrator will terminate the processes and notify the originator). The System Administrator then begins to shut down all subsystems in the order prescribed in the procedure below.

When all subsystems have been successfully shutdown, the UNIX prompt appears on the console screen. Total time from shutdown initiation to completion may be as long as 45 minutes.

### **Performing Normal Shutdown by Subsystem**

---

Steps A-G below are preliminary steps to shutting down each subsystem.

- A** Login to the server as **root**.
- B** Enter root password.
- C** Type **wall** and press **Return/Enter**.
- D** Type **This machine is being shutdown for *reason*. Please save your work and log off now. We are sorry for the inconvenience.** Press Control and D keys simultaneously.
- E** Wait at least five minutes.

- F** Type **shutdown -g0 -i0** or **shutdown now -i0** at the UNIX prompt and press **Return/Enter**.
- G** Power off all peripherals and the CPU.
- 1** Determine which machines perform the following functions:
- DNS Master
  - NIS Master
  - Mail Hub Server(s)
  - Automount Server
  - Clearcase Server
  - CSS
  - CLS
  - Other License Servers
  - MSS including Tivoli Server and Sybase SQL Servers
  - DSS
  - Ingest
  - PDPS
- 2** Power off the CLS server by following Steps A-G above for the machine. Once the system(s) have shutdown without error, proceed to Step 3.
- 3** Power off the PDPS server(s) by following Steps A-G above for each machine. Once the system(s) have shutdown without error, proceed to Step 4.
- 4** Power off the Ingest server(s) by following Steps A-G above for each machine. Once the system(s) have shutdown without error, proceed to Step 5.
- 5** Power off the DSS server(s) by following Steps A-G above for each machine. Once the system(s) have shutdown without error, proceed to Step 6.
- 6** Power off the MSS server(s) by following Steps A-G above for each machine. Once the system(s) have shutdown without error, proceed to Step 7.
- 7** Power off the Interface server(s) by following Steps A-G above for each machine. Once the system(s) have shutdown without error, proceed to Step 8.
- 8** Power off the Clearcase server(s) by following Steps A-G above for each machine. Once the system(s) have shutdown without error, proceed to Step 9.

- 9 Power off the CSS server, the NIS Master and the DNS Master by following Steps A-G above for each machine
- 

## Emergency Shutdown

An emergency shutdown is indicated when the System Administrator determines that the entire system or a component subsystem requires immediate maintenance. Indications that an emergency shutdown is in order include:

- The system or subsystem is locked up and users are unable to access or maneuver through the system
- An impending or actual power failure
- An actual system or subsystem hardware or software failure

Every effort should be made to minimize loss of data during an emergency shutdown by informing users to save files and log off if at all possible. However, circumstances may be such that a large-scale loss of data is unavoidable. In such instances, data will be restored from the most recent backup tapes and temporary backup files provided by the system (if applicable).

If the entire system is locked up then a complete system shutdown is required and the emergency shutdown and start-up procedures should be executed immediately. The DAAC manager is notified after the system has been brought back on line.

If major subsystems are locked up, a complete system shutdown is required and the emergency shutdown and start-up procedures should be executed immediately. The DAAC manager is notified after the system has been brought back on line.

If one or only a few of the subsystems are experiencing problems and only some of the users are affected, the subsystem problem(s) should be resolved first. If the System Administrator determines that all efforts to resolve the subsystem problems are exhausted and a shutdown is necessary, only the affected subsystems should be shutdown. Only if these steps provide no relief should the entire system be brought down. In any case, every effort should be made to accommodate users that are still on the system and to minimize data loss.

## Performing Emergency Shutdown

---

- 1 Login to the server as root.
- 2 Enter root password.
- 3 Type **sync** at the UNIX prompt then press **Return/Enter**.
  - **sync** causes all information in memory that should be on disk to be written out including modified super blocks, modified inodes, and delayed block I/O. If the system is to be stopped, sync must be called to insure file system integrity.

- 4 Type **sync** again at the UNIX prompt then press **Return/Enter**.
  - 5 Type **halt** at the UNIX prompt then press **Return/Enter**.
  - 6 Shutdown all client workstations.
  - 7 Determine which machines perform the following functions. Some machines may perform multiple functions:
    - Sybase SQL/Rep
    - Autosys
    - ClearCase
    - Automount
    - Mail Hub
    - NIS
    - DNS
  - 8 Power off the Sybase SQL/Rep server(s). Once the system has shutdown without error, proceed to Step 9.
  - 9 Power off the Autosys server(s). Once the system has shutdown without error, proceed to Step 10.
  - 10 Power off the ClearCase server(s). Once the system has shutdown without error, proceed to Step 11.
  - 11 Power off the Automount server(s). Once the system has shutdown without error, proceed to Step 12.
  - 12 Power off the NIS server(s). Once the system has shutdown without error, proceed to Step 13.
  - 13 Power off the DNS server(s).
- 

## System Shutdown by Server

In situations where only a single server requires maintenance, the System Administrator will need to determine if and how the faulty server affects other servers on the network. One server may be able to be shutdown without affecting the rest of the network, or several dependent servers may have to be shutdown in addition to the target server. Because of these interdependencies, each case will have to be uniquely evaluated.



This page intentionally left blank.

# Checking the Health and Status of the System

---

ECS is heavily dependent on the use of computer networks. Graphical tools available to monitor ECS status include a COTS program, **WhatsUp Gold**, two ECS programs, **ECS Assistant/ECS Monitor** and **EcMs-Whazzup??**, and a script **EcCsIdPingServers** that permits an operator to ping all servers. These programs provide system monitors with real-time status of the system and indications of potential problem areas.

## WhatsUp Gold

WhatsUp Gold (Version 7.03) is a graphical network monitoring application selected to monitor critical devices and services on the ECS Production Local Area Network (LAN) and/or additional ECS networks. It initiates alerts when it detects problems, and can send remote notifications by beeper, pager, and e-mail. It logs events to facilitate troubleshooting and reporting. It is implemented on Windows 2000 on a Personal Computer (PC) connected to the Production LAN. Detailed configuration and installation instructions are available in Document 914-TDA-246 *WhatsUp Gold 8.0 for the ECS Project, Release Notes*, and in the following vendor document:

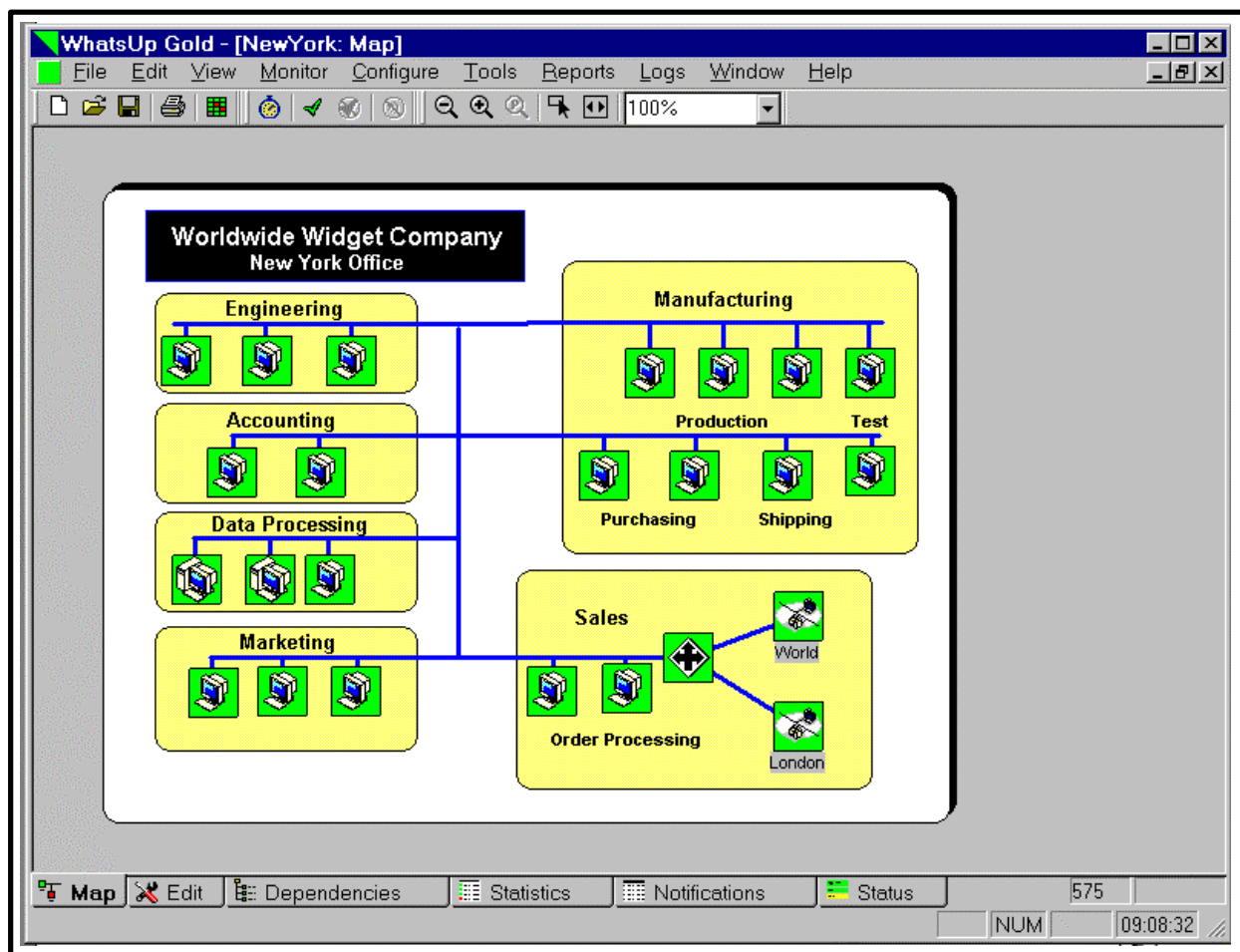
- *WhatsUp Gold version 8.0 User's Guide and Release Notes* accessible on the internet and downloadable at <http://support.ipswitch.com/kb/WG-20030121-DM01.htm>.

The instruction and procedures addressed here assume that the installation procedure specified in Document 914-TDA-246 has been executed. The specified procedure installs the WhatsUp Gold 8.0 application, creates a network map, sets up network map alert notifications, sets up a WinPopup notification message, sets up an SMTP (Simple Mail Transfer Protocol) e-mail notification message, sets the network map polling properties, sets device properties, saves the map, and starts WhatsUp Gold polling.

Once a network has been discovered by WhatsUp Gold, monitoring the state of the network can begin. Figure 1 shows the type of network map that the program creates for monitoring. Monitoring includes tasks such as checking the map for color alerts that indicate problems and checking for network changes.

## Launching WhatsUp Gold and Displaying the Network Map

As noted previously, the WhatsUp Gold application and graphical user interface (GUI) are installed and run in the Windows environment on a PC. Once the application is started and being used to monitor the network, it is typically left running at all times. This is because the application must be running with the network map open in order for its monitoring activities (i.e., polling and logging) to occur. Therefore, under normal circumstances, it will seldom be necessary to launch the application because it will be running continually. However, if something causes the application to be stopped (e.g., a failure of its host, or an inadvertent closure of the application), it will be necessary to start it again using the following procedure.



*Figure 1. WhatsUp Gold Network Map*

## Launching WhatsUp Gold and Displaying the Network Map

- 1 Execute the WhatsUpG.exe application in the Windows environment (e.g., double click on the **WhatsUpG** listing in a Windows Explorer window, or click on the **Start** button in the Windows taskbar and then click on the **Run . . .** option to open the **Run** dialog, from which you then enter the path for the **WhatsUpG.exe** application. A typical path is **c:\Program Files\WhatsUp\WhatsUpG.exe**, which may be entered or selected by clicking on the **Browse** button and navigating to the path. When the path is displayed in the **Open:** field of the **Run** dialog, click on the **OK** button.).
  - The **WhatsUp Gold** window is opened.
- 2 Follow menu path **F**ile→**O**pen.
  - The **Open** dialog box is displayed.

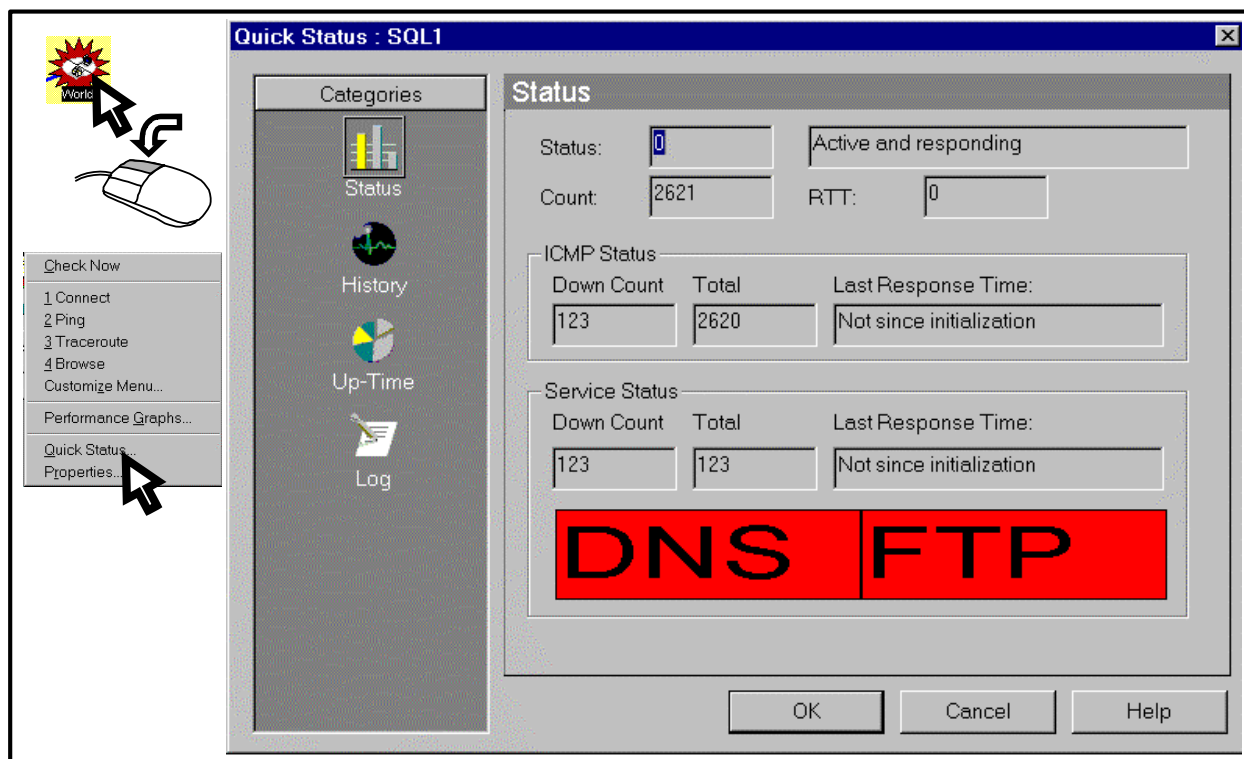
- 3 Double click on the name of your network map, or select the name with a single click and then click on the **Open** button.
    - The network map is displayed and polling begins.
- 

### **Responding to Color Alerts and Obtaining Status of a Node**

Objects that have an abnormal condition can be identified by a change in appearance on the network map. Colors may be changed, but the following default conventions apply in a map window to indicate the status of a device or service:

- Device name highlighted: indicates that WhatsUp Gold has recorded an event for the device in a log.
- Device icon on a green square background: indicates that the device is up (i.e., responds to polling).
- Device icon on a light green diamond-shaped background: indicates that the device has missed at least one polling request.
- Device icon on a yellow diamond-shaped background: indicates that the device has missed two polling requests.
- Device icon on a red elongated diamond-shaped background: indicates that the device is down (i.e., is not accessible or has missed four consecutive polling requests). Once the device has missed eight polling requests, the background is changed to a dark red starburst.
- Device icon on a light purple octagon-shaped background: indicates that a standard service on the device is down.
- Device on a gray square background: indicates monitoring has been turned off for the device.

A color alert on a symbol indicates that some part of that object may have problems. To help isolate a fault on the network, it is possible to click with the right (or non-preferred) mouse button on the symbol with the color alert and bring up a status display that provides the overall status of the node based on TCP/IP polling, the Internet Control Message Protocol (ICMP) status, and the status of services on the node. Figure 2 shows an example of a status display for a node that is active and responding to polling but on which the DNS and FTP services are down (indicated in red).



**Figure 2. WhatsUp Gold Quick Status Display for a Node**

The following procedure is applicable for obtaining and reviewing the WhatsUp Gold **Quick Status** display for a node. It includes a step for acknowledging the alert that prompted calling the status display. This acknowledgement prevents additional instances of the alert on the node unless the alert is specifically configured to be sent regardless of the acknowledgement.

### **Responding to a Color Alert and Obtaining the Status of a Node**

- 1 With the network map open, use the right (or non-preferred) mouse button to click on the icon for the node showing a color alert (i.e., the node label is highlighted if there has been an entry in the Event Log related to the alert and the background is other than a green square or whatever you have selected as the indication for normal status).
  - A popup menu is displayed.
- 2 On the popup menu, click on **Quick Status . . .**.
  - The **Quick Status** dialog box for the selected node is displayed showing the **Status** (including a device status code of 0 to indicate that the device is up or other value to indicate an error, the text of an error message, and information about device polling, ICMP status, and a graph showing any monitored services in green if they are up or

red if they are down) and providing access to charts of polling **History** and **Up-Time**. It also provides access to a **Log** display of any service or device “up” or “down” events for the selected node.

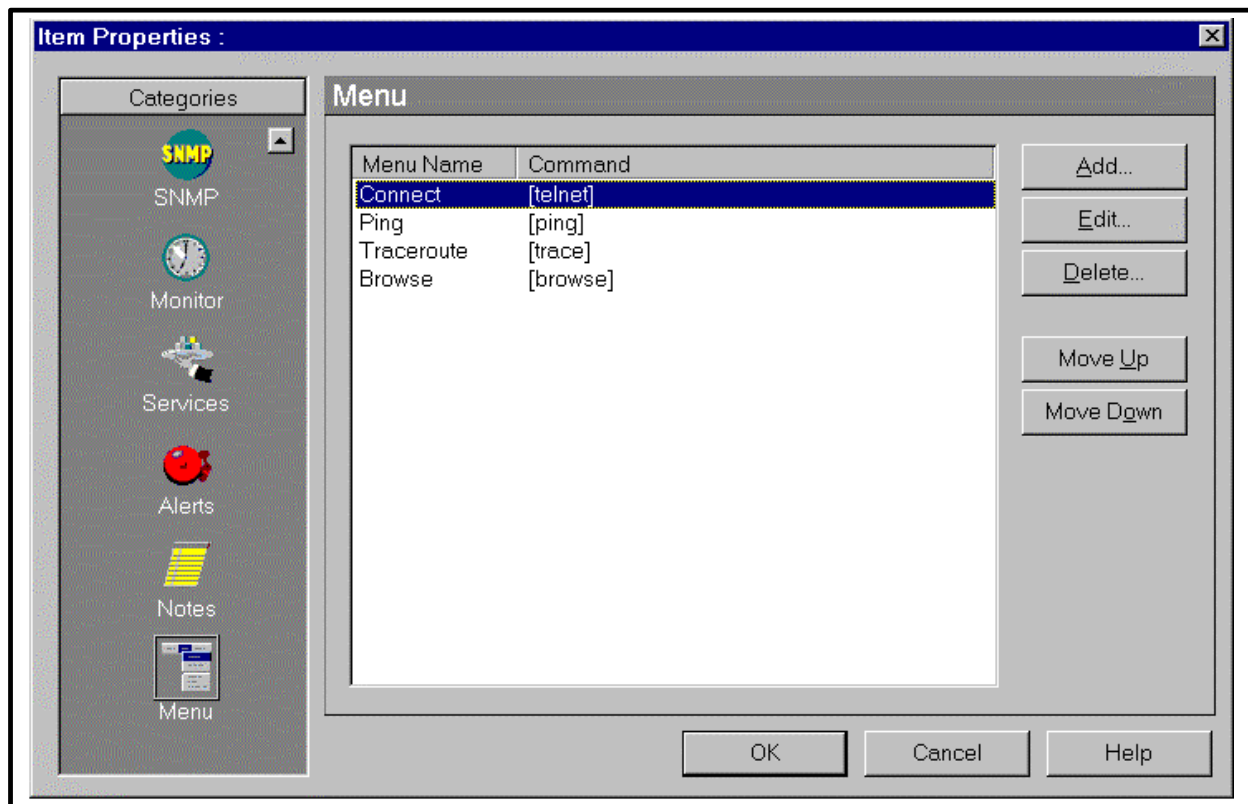
- 3 Review the status information and, in the left frame, click as desired on **History**, **Up-Time**, **Log**, or **Status** to display or re-display information in those categories.
  - 4 Click on the **OK** button to dismiss the **Quick Status** dialog.
    - The **Quick Status** dialog is closed.
  - 5 To acknowledge the alert, follow menu path **Monitor→Acknowledge**.
    - The highlighting is removed from the node label and additional instances of the alert on the node are prevented (unless the alert has been configured to be sent regardless of the acknowledgement – see **User’s Guide**).
- 

### Configuring a Popup Menu for a Node or Multiple Nodes

The popup menu accessible using the right (or non-preferred) mouse button to click on a node on a network map (see Figure 2) typically includes the following choices:

- **Check Now** – initiate a single poll of the network.
- **1 Connect** – open a telnet session on the device represented by the node on the map.
- **2 Ping** – start the Ping tool to send ICMP packets to the device and view the results.
- **3 Traceroute** – start the Traceroute tool to examine the network path and the intervening routers from the WhatsUp Gold machine to the device.
- **4 Browse** – start the default browser using the IP address as the URL.
- **Customize Menu . . .** – open the **Item Properties** dialog box to permit adding, editing, deleting, or moving items on the popup menu.
- **Performance Graphs** – open **Report Job Properties** and **WhatsUp Gold Performance Graphs** dialogs to permit selecting and preparing performance reports and graphs.
- **SNMP View . . .** – start the SNMP View tool using the device’s IP address. The SNMP View tool lets you read SNMP data on the device. This command appears only if the SNMP Manageable option (on the Device Properties (SNMP)) is selected.
- **Quick Status . . .** – open the **Quick Status** dialog to provide access to status, history, up-time, and log information for the device.
- **Properties . . .** – open the **Item Properties** dialog box to permit setting parameters for the device, including General functions, monitoring functions, services, alerts, and other categories (see **User’s Guide**).

The popup menu may be configured or customized by selecting **Customize Menu . . .**. This opens the **Item Properties** dialog box illustrated in Figure 3.



**Figure 3. WhatsUp Gold Item Properties Dialog Box**

The following procedure is applicable.

### **Configuring the Popup Menu for a Node or Multiple Nodes**

---

- 1 On the network map, select the node(s) for which the popup menu is to be configured. If more than one node is to be selected, use shift-click (i.e., hold down the shift key and click sequentially on the nodes to be selected) or click-drag (i.e., hold down the mouse button and drag diagonally to outline a rectangle enclosing the items to be selected, releasing the button when the items are enclosed).
  - The selected nodes are indicated by the appearance of small white squares at the corners.
- 2 Use the right (or non-preferred) mouse button to click on the selected node (or one of the selected nodes).
  - A popup menu is displayed.

- 3 On the popup menu, click on **Customize Menu . . .** (for one node) or **Add Custom Menus to Selected Devices . . .** (for multiple nodes).
  - If one node was selected, the **Item Properties** dialog box is displayed to permit customization of the menu for that node. (*Note:* It is also possible to display this box for one node by selecting **Properties** from the popup menu and then clicking on **Menu** in the left frame of the resulting **Item Properties** dialog.)
  - If more than one node was selected, the **Add to Selected Devices** dialog box is displayed to permit customization of the menus for the selected nodes. This box is similar to the **Item Properties: Menu** dialog, but menu items on any of the selected nodes appear in the dialog box, with a check box next to each item. For an item that is on all selected nodes, the check box is white and displays a check mark; for an item that is assigned to some but not all of the selected nodes, the check box is gray and displays a check mark.
- 4 To add a menu item, click on the **Add** button.
  - The **Edit Menu Item** dialog box is displayed with three empty fields: (1) **Menu name:**; (2) **Command:**; and (3) **Arguments:**. Using this box, it is possible to create a menu item for starting a program when the item is chosen. The **Menu name:** field is used to specify the name of the menu item that will appear in the popup menu. The **Command:** field is used to enter the (file)name of any executable program to be started when the menu item is chosen from the popup menu. The **Arguments:** field is used to pass parameters to the specified program. See the **User's Guide** for detailed information on establishing and using popup menu items to run programs.
- 5 To select a displayed menu item for editing or moving, click on the menu item in the list.
  - The selected item is highlighted.
- 6 To edit a selected item, click on the **Edit** button.
  - The **Edit Menu Item** dialog box is displayed as in Step 4, with information for the selected item displayed in its three fields. The displayed data may be edited to change the menu display and/or actions (see **User's Guide**).
- 7 To move a selected item up or down in the list, click on the **Move Up** or **Move Down** button as appropriate.
  - The selected item is moved up or down in the list as the button is clicked.
- 8 To delete a selected item for a single node, using the **Item Properties** dialog box, click on the **Delete** button.
  - A confirmation dialog is displayed to ensure that you would like to remove the item; click on the **Yes** button to confirm.



- 9 For multiple nodes, to delete an item from the popup menu for all selected nodes, using the **Add to Selected Devices** dialog, click repeatedly on the accompanying checkbox until the check mark is removed.
    - The check box is empty.
  - 10 For multiple nodes, to assign a menu item to all of the selected nodes, using the **Add to Selected Devices** dialog, click repeatedly on the accompanying checkbox until the check mark is displayed in a white (i.e., not gray) box.
    - The checkbox is white and the check mark is displayed.
  - 11 Click on the **OK** button.
    - The menu changes are applied and the **Item Properties** or **Add to Selected Devices** dialog is closed.
- 

## Using Network Tools

WhatsUp Gold provides a set of tools to display a variety of information about nodes on the network. These tools are displayed on tabs, with the parameters and results area for one tool on each tab. The tools include:

- **Info** – display a summary of device information.
- **Time** – synchronize your computer's clock with a remote time server.
- **HTML** – query a web address.
- **Ping** – verify connectivity to a host.
- **TraceRoute** – Trace and view the route to an Internet host.
- **Lookup** – query Internet domain name servers for information about hosts and name servers.
- **Finger** – display information about users on a host.
- **Whois** – display information from the network information center about Internet domain ownership and Internet groups.
- **LDAP** – (Lightweight Directory Access Protocol); search directories for names and information stored in an LDAP directory on another computer.
- **Quote** – view quotations from a quote server.
- **Scan** – scan a range of IP addresses to create a network map.
- **SNMP** – view and graph Simple Network Management Protocol (SNMP) values for a device.

- **WinNet** – View Windows Network domains, hosts, and workstations.
- **Throughput** – test data throughput on the connection between your computer and a remote computer.
- **System Info** – view information about your local system.

Not all of these tools are necessarily appropriate for ECS use, but the **WhatsUp Gold User's Guide** provides detailed information on all of them. This lesson presents information on just three of them.

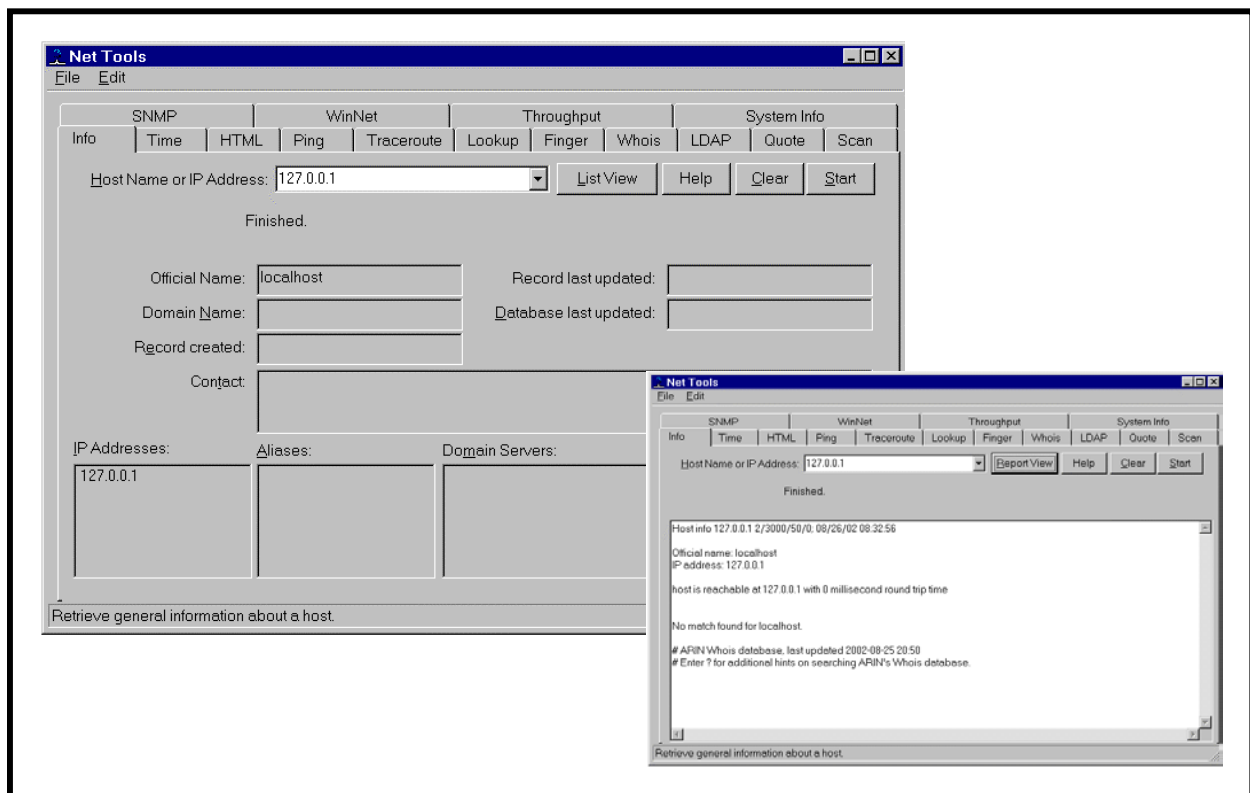
The **Info** tool, illustrated in Figure 4, displays a summary of information about a network host or device, including the official host name, IP address, and contact information. An Info request on a host name also pings the host to verify connectivity.

The following procedure is applicable for using the Net Tools Info Tool to obtain information on a node.

#### **Use the Net Tools Info Tool to Obtain Information on a Node**

---

- 1 Follow menu path **T**ools→**I**nter Tools.
  - The **Net Tools** window is displayed.
- 2 If necessary, click on the **Info** tab to access the **Info** tab display (when the **Net Tools** window is opened, WhatsUp Gold displays the tab most recently accessed).
  - The **Info** tab controls and fields are displayed.
- 3 In the **Host Name or IP Address:** field, type the name or IP address of the host to be queried (this must be a fully qualified host name or address).
  - The typed entry is displayed in the field.
- 4 Click on the **S**tart button.
  - A **Searching . . .** indicator appears and the **S**tart button toggles to **S**top to show that the query is in progress. At any time during the query, a click on the **S**top button stops the query.



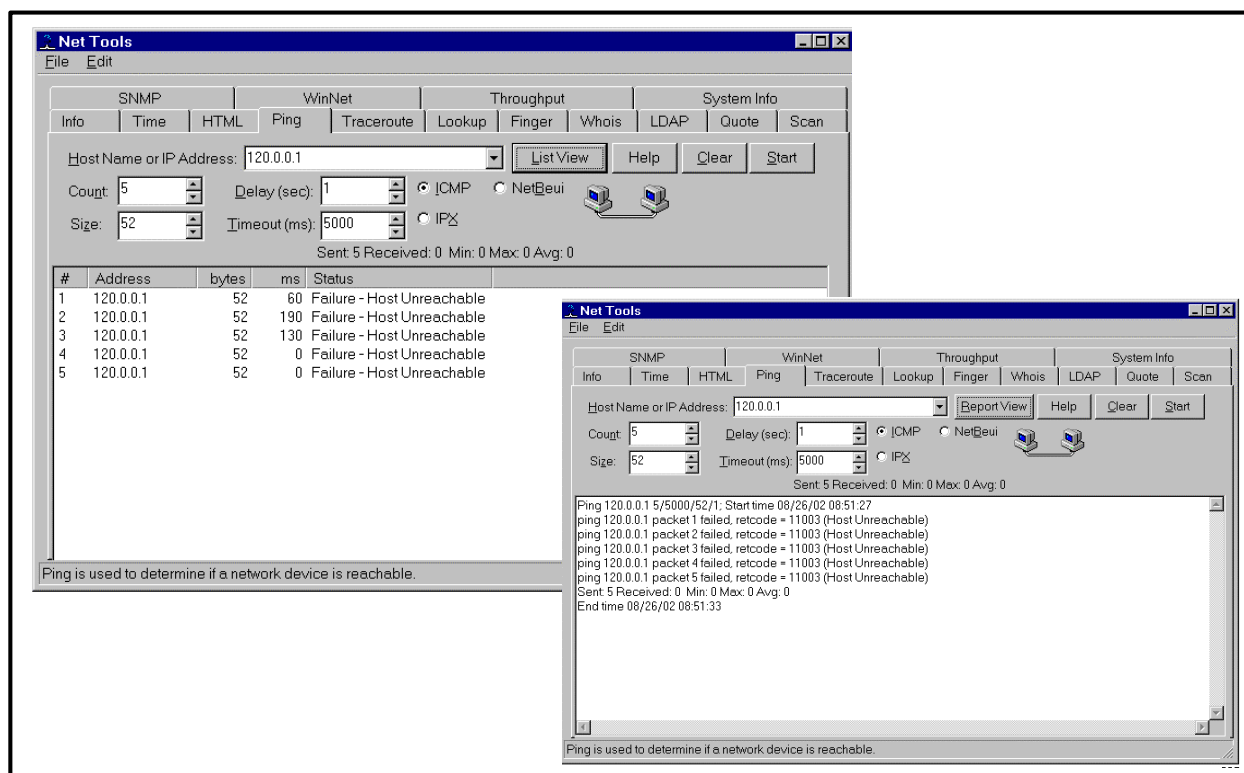
**Figure 4. WhatsUp Gold Net Tools - Info Tool**

- The results of the query are displayed. (A click on the **Clear** button erases the results from the display window.) The **List View/Report View** button permits toggling between the Report View and the List View of the results. The Report View is a summary showing:
  - Official Name.
  - Domain Name.
  - Date the record was created.
  - Date the record was last updated.
  - Date the database was last updated.
  - Contact information (from the Whois database).
  - IP Addresses and Domain Servers.

The List View is a detailed list of the obtained information, including the results of the ping and more extensive information on the query.

The **Ping** tool, illustrated in Figure 5, is a network diagnostic tool used to verify connectivity to a selected system on the network. This tool sends a data packet (an ICMP “echo request”) to a remote host and displays the results for each “echo reply.” This pinging command also displays the time for a response to arrive in milliseconds, as well as debugging information about the network interface. Multiple instances of the **Ping** tool may be active simultaneously.

The use of the **Ping** tool provides a quick way to verify that a device is not functioning. If the ping operations do not produce any responses or they time out, then the node is probably down or otherwise unreachable over the network.



**Figure 5. WhatsUp Gold Net Tools - Ping Tool**

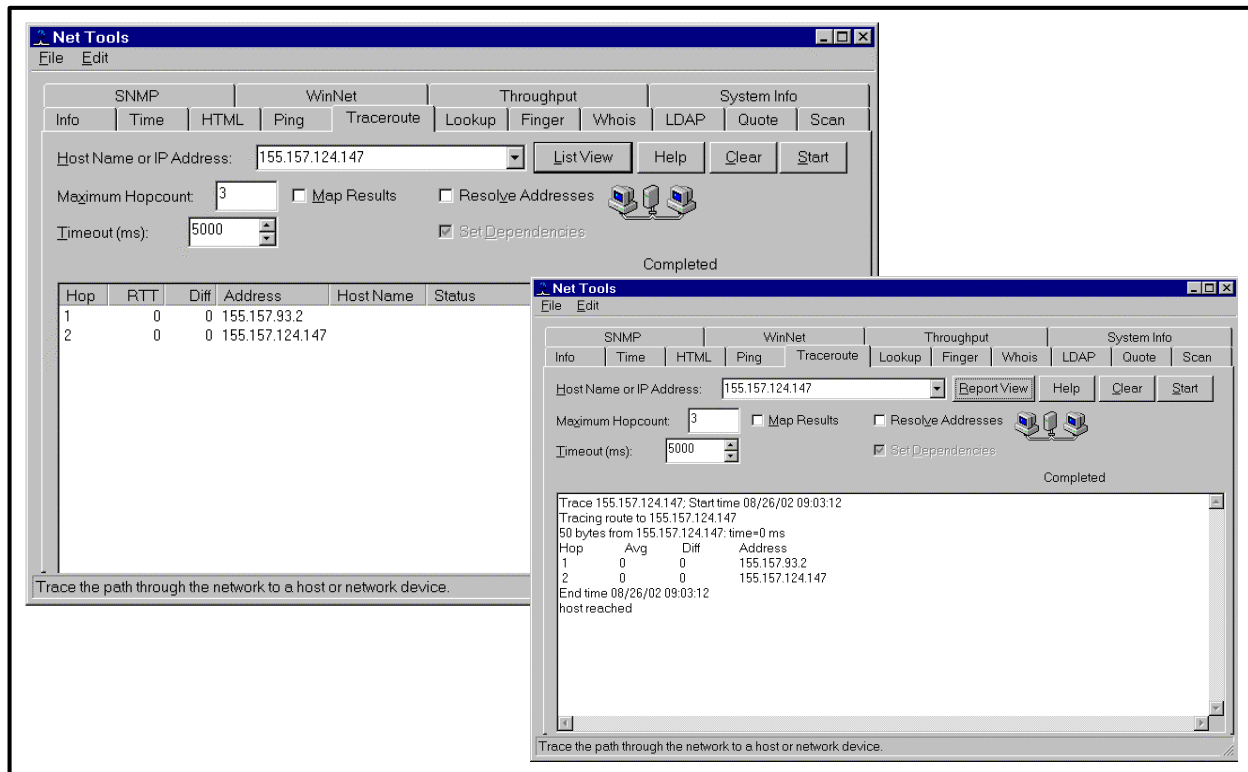
The following procedure is applicable for using the Net Tools Ping Tool to verify connectivity on a node.

### **Use the Net Tools Ping Tool to Verify Connectivity on a Node**

- 1 Follow menu path **T**ools→**N**et Tools. . .
  - The **Net Tools** window is displayed.

- 2 If necessary, click on the **Ping** tab to access the **Ping** tab display (when the **Net Tools** window is opened, WhatsUp Gold displays the tab most recently accessed).
    - The **Ping** tab controls and fields are displayed.
  - 3 In the **Host Name or IP Address:** field, type the name or IP address of the host to be checked (this must be a fully qualified host name or address).
    - The typed entry is displayed in the field.
  - 4 Click one of the radio buttons below the **Host Name or IP Address:** field to specify the protocol to use for ping (use **ICMP** for TCP/IP hosts, **IPX** for Novell NetWare hosts, or **NetBEUI** for Windows network hosts).
    - The selected radio button is filled to indicate the specified protocol.
    - *Note:* To ping an IPX device, Microsoft's NWLink IPX/SPX Compatible Transport must be installed and running on the WhatsUp Gold system (see "System Requirements" in the **User's Guide**).
  - 5 If it is desired to change the default number of pings to be sent, click at the end of the **Count:** field.
    - The cursor is displayed at the end of the **Count:** field.
  - 6 To set a new value for **Count:**, use the **Backspace** key to remove the current value, and type the new value.
    - The typed value appears in the **Count:** field.
  - 7 Repeat Steps 5 - 6 for other options you wish to change, substituting **Delay (sec.):**, **Size**, or **Timeout (ms):** for the field name of the option to be changed, specifying respectively the number of seconds to wait between pings, the length in bytes of each packet to be sent by the **Ping** command, and the number of milliseconds of non-response from the host to be considered a failure of the ping.
  - 8 Click on the **Start** button.
    - The **Start** button toggles to **Stop** to show that the ping operation is in progress. At any time during the operation, a click on the **Stop** button stops the ping.
    - The display field at the bottom of the window shows the results of the pings. (A click on the **Clear** button erases the results from the display window.) The **List View/Report View** button permits toggling between the Report View and the List View of the results. The Report View provides, for each ping as it occurs, the address, the number of bytes sent, the response time, and the status. The List View lists the pings, the result for each packet, and the retry code.
-

The **Traceroute** tool, illustrated in Figure 6, permits the operator to trace and view the route an IP packet follows from the local host to another host on the network. Response times are displayed in milliseconds and vary depending on network load. **Traceroute** can be helpful for finding potential trouble spots on large and complex networks that are connected by routers. The results of a traceroute operation can be displayed on a network map.



**Figure 6. WhatsUp Gold Net Tools Traceroute Tool**

The following procedure is applicable for using the Net Tools Traceroute Tool to trace a route.

### **Using the Net Tools Traceroute Tool to Trace a Route**

- 1 Follow menu path **T**ools→**N**et Tools. . .
  - The **Net Tools** window is displayed.
- 2 If necessary, click on the **Traceroute** tab to access the **Traceroute** tab display (when the **Net Tools** window is opened, WhatsUp Gold displays the tab most recently accessed).
  - The **Traceroute** tab controls and fields are displayed.

- 3 In the **Host Name or IP Address:** field, type the name or IP address of the host to which the route is to be traced (this must be a fully qualified host name or address).
  - The typed entry is displayed in the field.
- 4 If it is desired to change the maximum number of hops to trace before ending the traceroute operation (a “hop” is the passing of an IP packet from one host to another), click at the end of the **Maximum Hopcount:** field.
  - The cursor is displayed at the end of the **Maximum Hopcount:** field.
- 5 To set a new value for **Maximum Hopcount:** use the **Backspace** key to remove the current value, and type the new value.
  - The typed value appears in the **Maximum Hopcount:** field.
- 6 If it is desired to change the number of milliseconds of non-response from the host to cause the Traceroute to fail, click at the end of the **Timeout (ms):** field.
  - The cursor is displayed at the end of the **Timeout (ms):** field.
- 7 To set a new value for **Timeout (ms):** use the **Backspace** key to remove the current value, and type the new value.
  - The typed value appears in the **Timeout (ms):** field.
- 8 If it is desired to specify that WhatsUp Gold is to map the results of the Traceroute operation, click on the **Map Results** checkbox.
  - The clicked box displays a checkmark to indicate its selection, and when **Traceroute** is run, the route will be drawn on the network map, displaying an icon for each router and showing the connections from router to router until it reaches the host.
- 9 If it is desired to specify that the host names of all routers along the route be displayed along with the IP addresses, click on the **Resolve Addresses** checkbox.
  - The clicked box displays a checkmark to indicate its selection, and when **Traceroute** is run, the host names as well as the IP addresses will be shown for each router (instead of just the IP addresses). This will add time to the Traceroute operation to resolve the IP addresses.
- 10 If **Map Results** is checked and it is desirable to set dependencies such that each router found is to be set as an “up” dependency on the previous router in the route, click on the **Set Dependencies** checkbox. This choice is only available when **Map Results** is checked. It means that when WhatsUp Gold polling finds a router down, it will not poll routers further along the route to a host.
  - The clicked box displays a checkmark to indicate its selection, and when **Traceroute** is run, each router found will be set as an “up” dependency on the previous router in the route.

## 11 Click on the **Start** button.

- An indicator shows the Traceroute operation in progress and the **Start** button toggles to **Stop** to show that the operation is in progress. At any time during the operation, a click on the **Stop** button stops the tracing.
  - The display field at the bottom of the window shows the results of the traceroute operation. (A click on the **Clear** button erases the results from the display window.) The **List View/Report View** button permits toggling between the Report View and the List View of the results. The Report View provides for each hop as it occurs the address, the response time or Round Trip Time (RTT), and the status. The List View lists the hops, addresses, and more detailed information on the tracing of the route.
- 

## Using WhatsUp Gold Logs

WhatsUp Gold captures data in four types of logs:

- **Syslog** – logs standard UDP messages sent from devices (e.g., routers, switches, UNIX hosts).
- **Event Log** – logs events (changes to network status, such as a device going down or a device coming back up). The Event Log provides a history of what has occurred on the network. An associated **Debug Log** window permits viewing events as they occur.
- **Statistics Log** – records polling statistics (accumulated round trip times, or RTT, of polls sent to a device) to measure the availability and performance of a device.
- **SNMP Trap Log** – displays all SNMP traps that have been received. To enable SNMP traps, the SNMP trap handler must be specifically enabled (refer to **User's Guide**).


Detailed information on the nature of the logged data and the log designations is provided in the **User's Guide**. The **User's Guide** also describes how to change the way events are logged, and how to create reports and graphs using the logged data to show the status of the network in several ways (e.g., performance graphs, event reports, and statistics reports). The Event Log, described here, can be a useful initial troubleshooting tool.

The Event Log stores data in weekly file increments with the following file format: **EV-yyyy-mm-dd.tab**. The log automatically records application-level events (e.g., a device or service going down) for devices that have **Enable Logging** selected in the **Alerts** dialog box. After sufficient event data logging, the data can be used to generate reports. The data can also be saved in a tab-delimited file that can be imported to another application, such as a spreadsheet program. It may also be useful just to view the Event Log for information related to an observed problem. For example, if the network map shows a color alert for a device and the device does not respond to a ping, the Event Log may provide additional information concerning the time the device went down and a message addressing the problem. Use the following procedure for reviewing the WhatsUp Gold Event Log.



## Reviewing the WhatsUp Gold Event Log

---

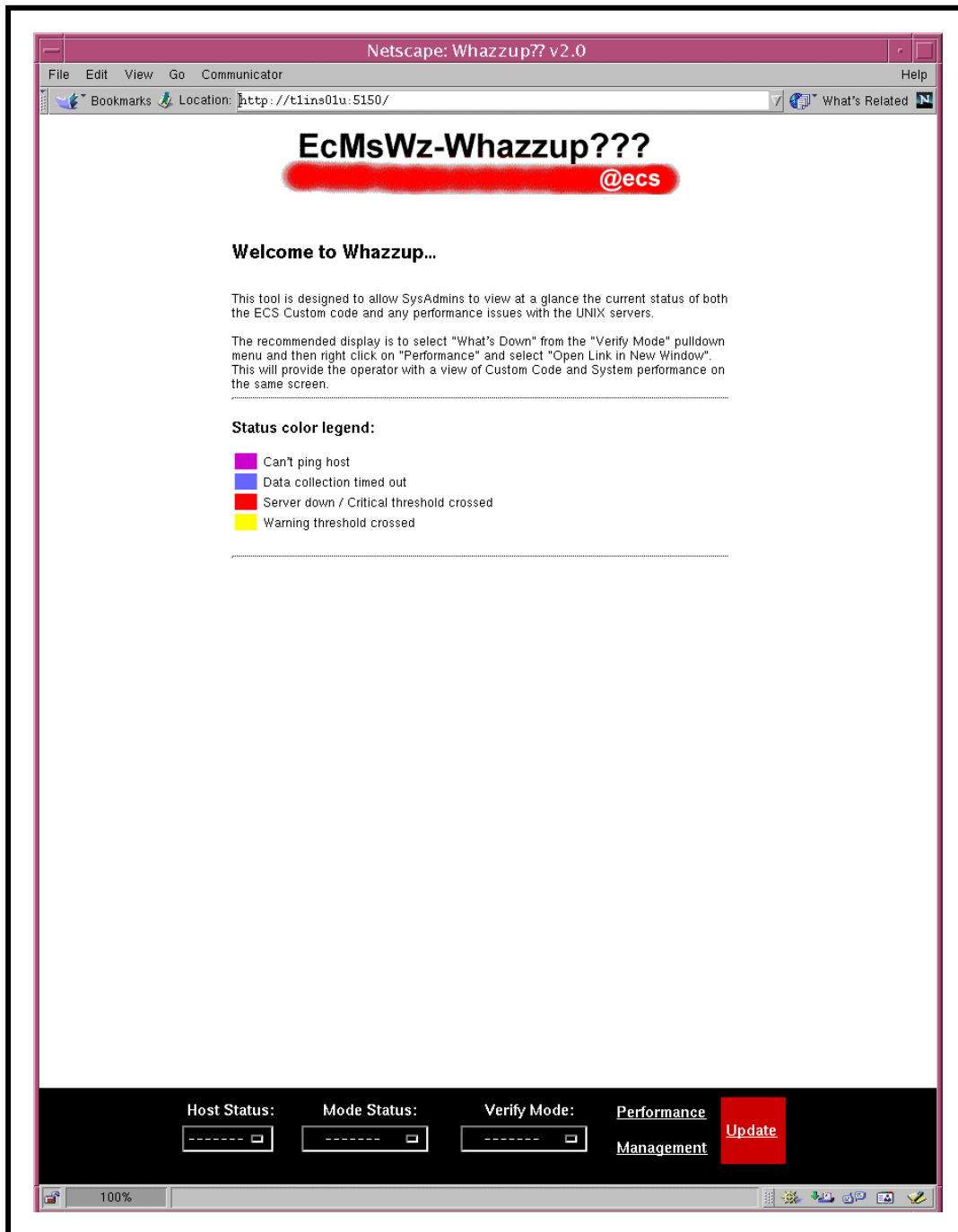
- 1 Follow menu path **Logs**→**Event Log**.
    - The **Event Logs** - *<date range>* window is displayed. *Note:* The date range is the current week, and the events are displayed in raw format (the **Raw** radio button is filled to indicate its selection) with the most recent first. It is possible to click on the **Formatted** radio button to select a display showing the date and time information in *mm/dd/yyyy* and *hh:mm:ss* format, with column headers that can be clicked to sort the list by date, time, or message.
  - 2 Review the list of events to locate a message identifying an **Alert** or **DOWN** event for any device that has shown a color alert on the network map or that has failed to respond to pinging.
    - The message provides the date and time of the event, as well as specific information in the message concerning the type of event.
  - 3 If it is desirable to view events from the prior week, click on the **Back** icon ().
    - The events from the previous week are displayed. *Note:* The date range specifies the prior week, and the events are displayed in the currently selected format (raw or formatted) with the most recent first. There are other icons: a **Filter** icon (or menu equivalent) permits customizing the log viewer to show logs in a different time span other than weekly; a **Find** icon permits locating text in the display; a **Print** icon permits printing the contents of the display; and other navigation icons permit moving to specific ranges of events for display. The **User's Guide** provides detailed guidance on navigating and locating text in the Event Log display.
  - 4 If it is desirable to print the contents of the display, click on the **Print** icon.
    - The **Print** dialog box is displayed, permitting specification of a printer, print range, and number of copies.
- 

## Whazzup???

A powerful COTS program modified for ECS and used to monitor the ECS system is EcMsWz - Whazzup. It is a web-accessed program that provides a graphical display of Host Status, Mode Status, Mode Verification and Performance Management. Figure 7 shows the initial Whazzup display.

These functions of Whazzup provide graphical displays of host and software-server status in real-time mode. When used in conjunction with Tivoli and ECS Assistant, System Administrators can acquire a comprehensive knowledge of the system's status.

To start EcMsWz-Whazzup, execute the following procedure:



**Figure 7. ECS Whazzup Initial Display**

## Starting EcMsWz-Whazzup

---

- 1 Logon onto a host machine.
  - 2 At the UNIX prompt on the host from which Whazzup is to be run, type **setenv DISPLAY <hostname>:0.0** then press **Return/Enter**. Note: If the host has been remotely accessed via ssh then do not use the setenv DISPLAY command again. Doing so will compromise system security.
    - The hostname is the name of the machine on which Whazzup is to be displayed, i.e., the machine you are using.
    - To verify the setting, type **echo \$DISPLAY** then press **Return/Enter**.
  - 3 At the UNIX prompt, using secure shell, log on to the Whazzup host, xxins0x. Type **ssh xxins0x** then press **Return/Enter**.
  - 4 Enter your **passphrase** then press **Return/Enter**.
    - You are logged into the Whazzup host machine.
  - 5 Start the Netscape web browser by typing **netscape &** then press **Return/Enter**.
    - You are in the web browser on the Whazzup host xxins0x.
  - 6 Type in the URL to activate Whazzup. Enter **http://xxins0x:5150**.
    - The Whazzup intro screen appears (Figure 7).
  - 7 Select a monitoring function
    - **Host Status** to determine individual host parameters.
    - **Mode Status** to determine “up” servers for the selected Mode.
    - **Verify Mode** to determine status of all servers for a selected Mode.
    - **Performance Management** to determine the performance status all hardware/software servers for all modes.
- 

### Host Status

Selecting Host Status provides a pop-up box (Figure 8) from which to choose a specific host to determine its status.

Host Status data include percent of CPU used, Swap Free space, Memory Free space, and Server information. (Figure 9)

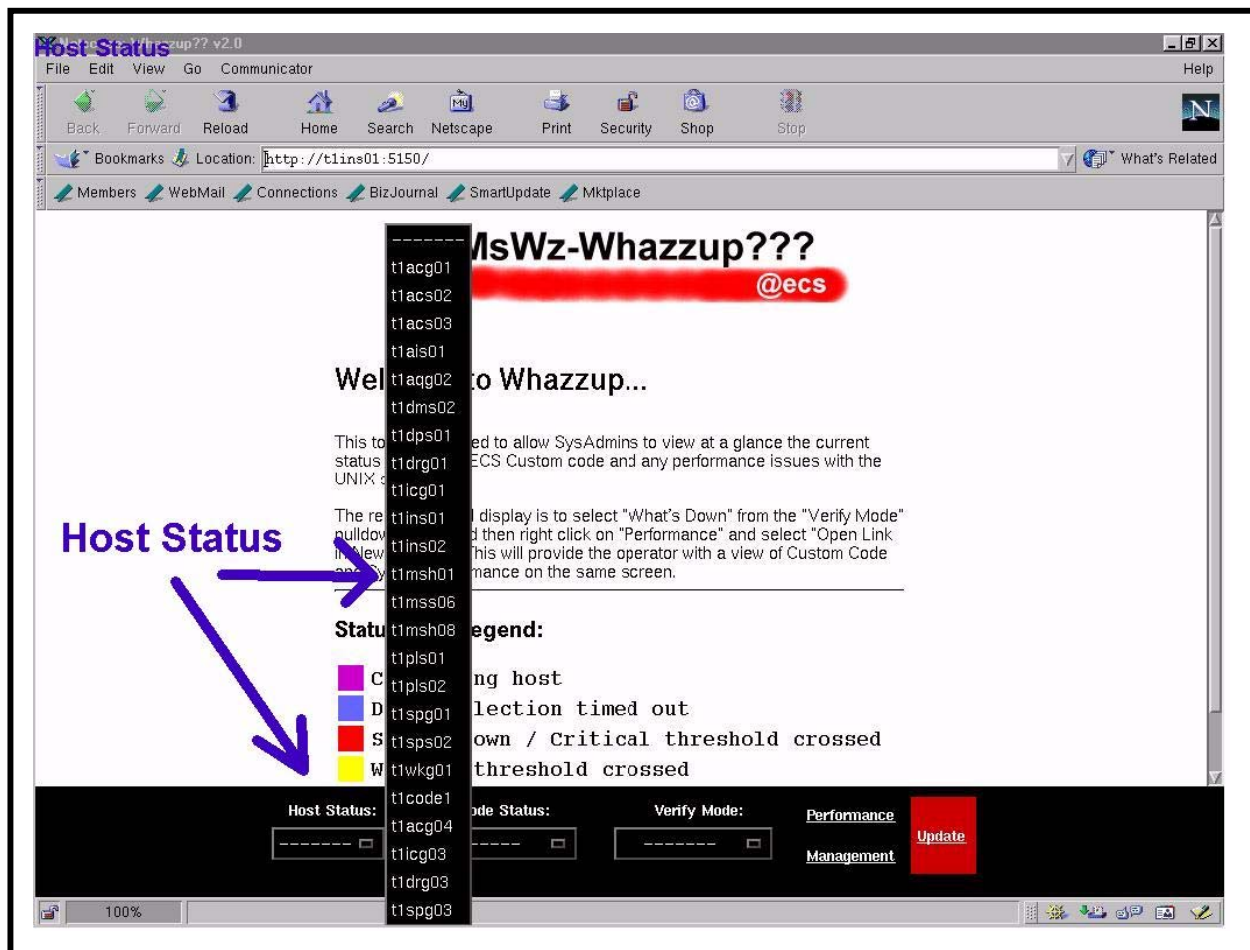
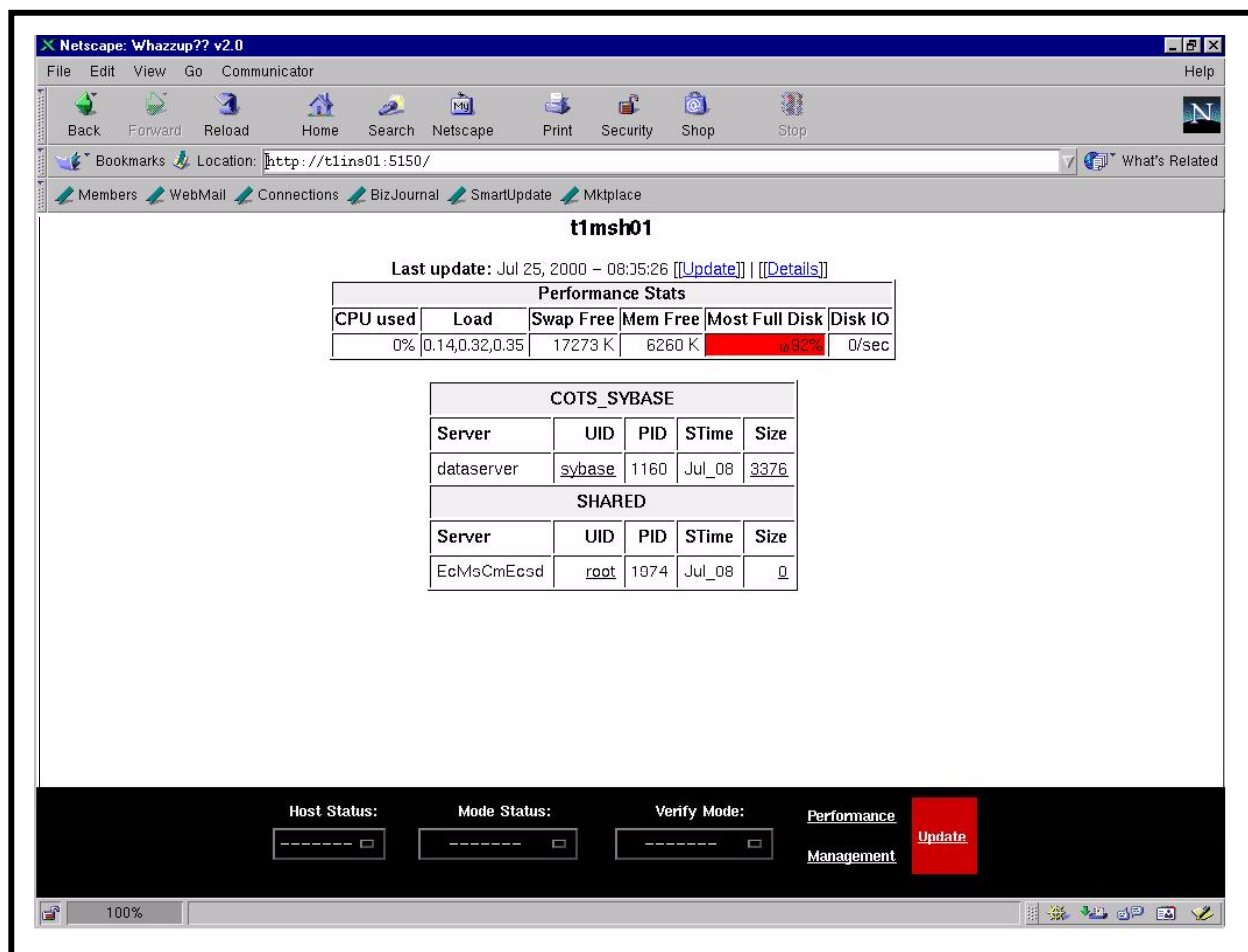
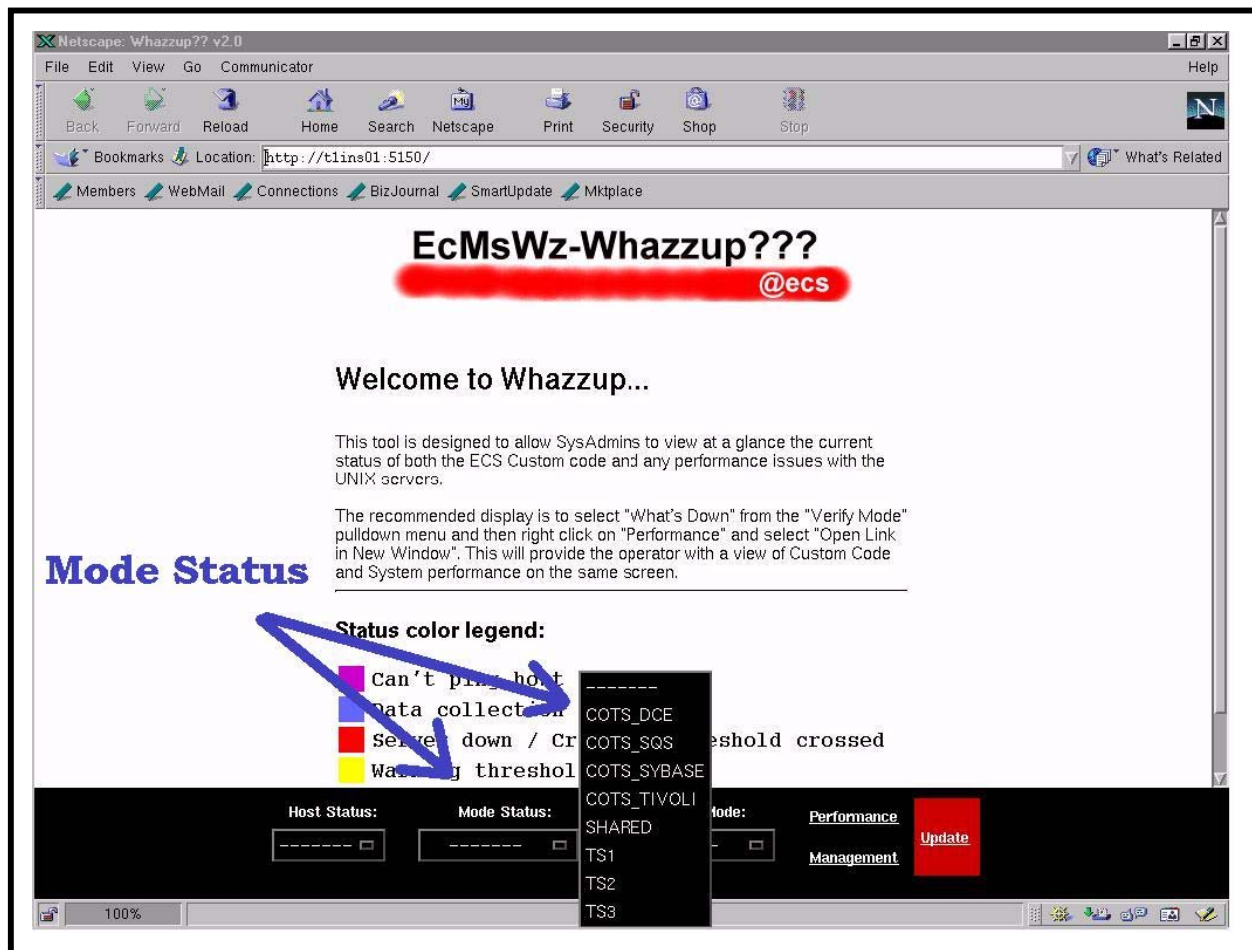


Figure 8. Host Status Pop-Up Display

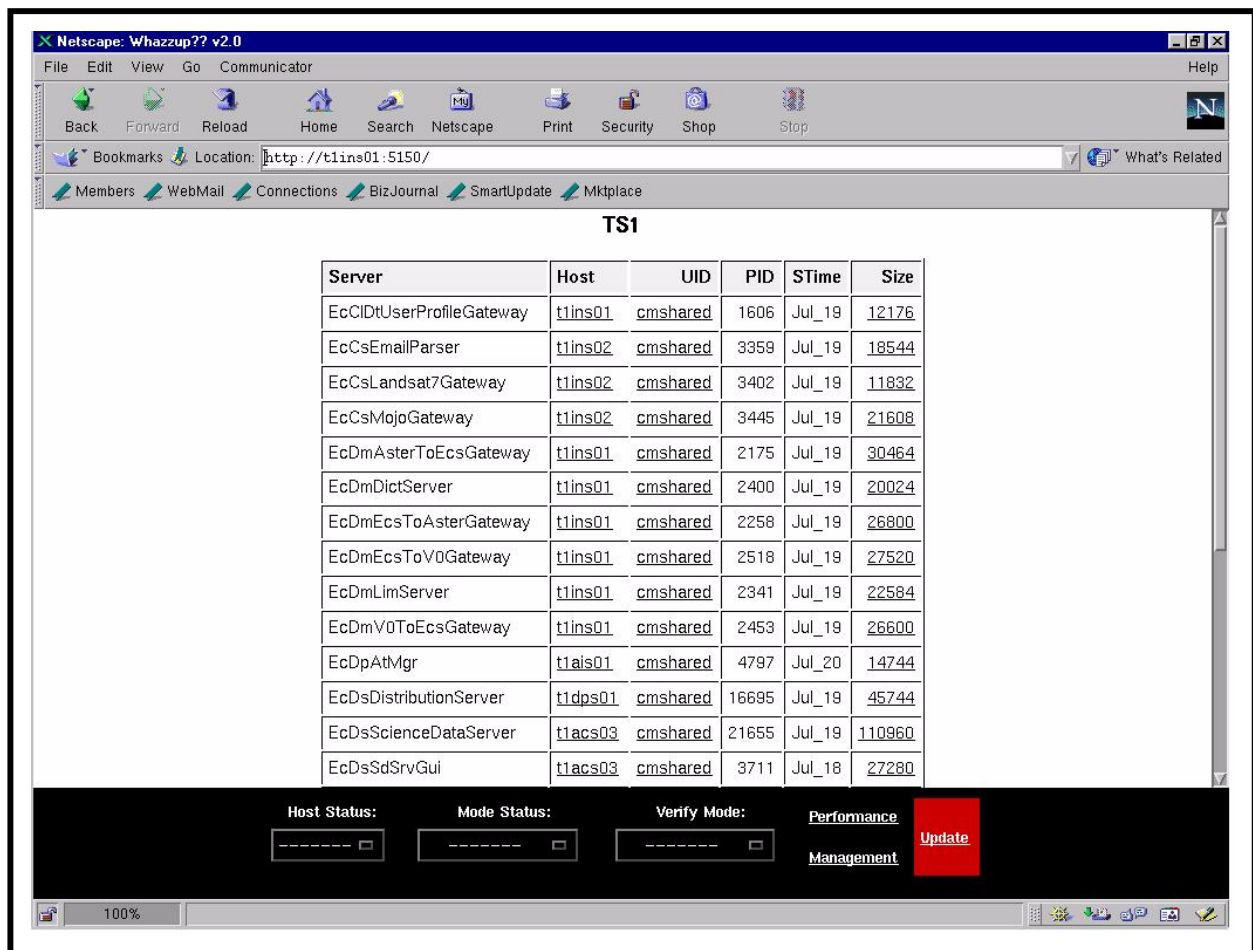


**Figure 9. Host Status Data Display**

Selecting Mode Status (Figure 10) enables a pop-up window showing Modes available. Subsequent to selecting the desired Mode, a display of “up” ECS Servers is provided as shown in Figure 11.



**Figure 10. Mode Status Pop-Up Display**



**Figure 11. Mode Status Data Display**

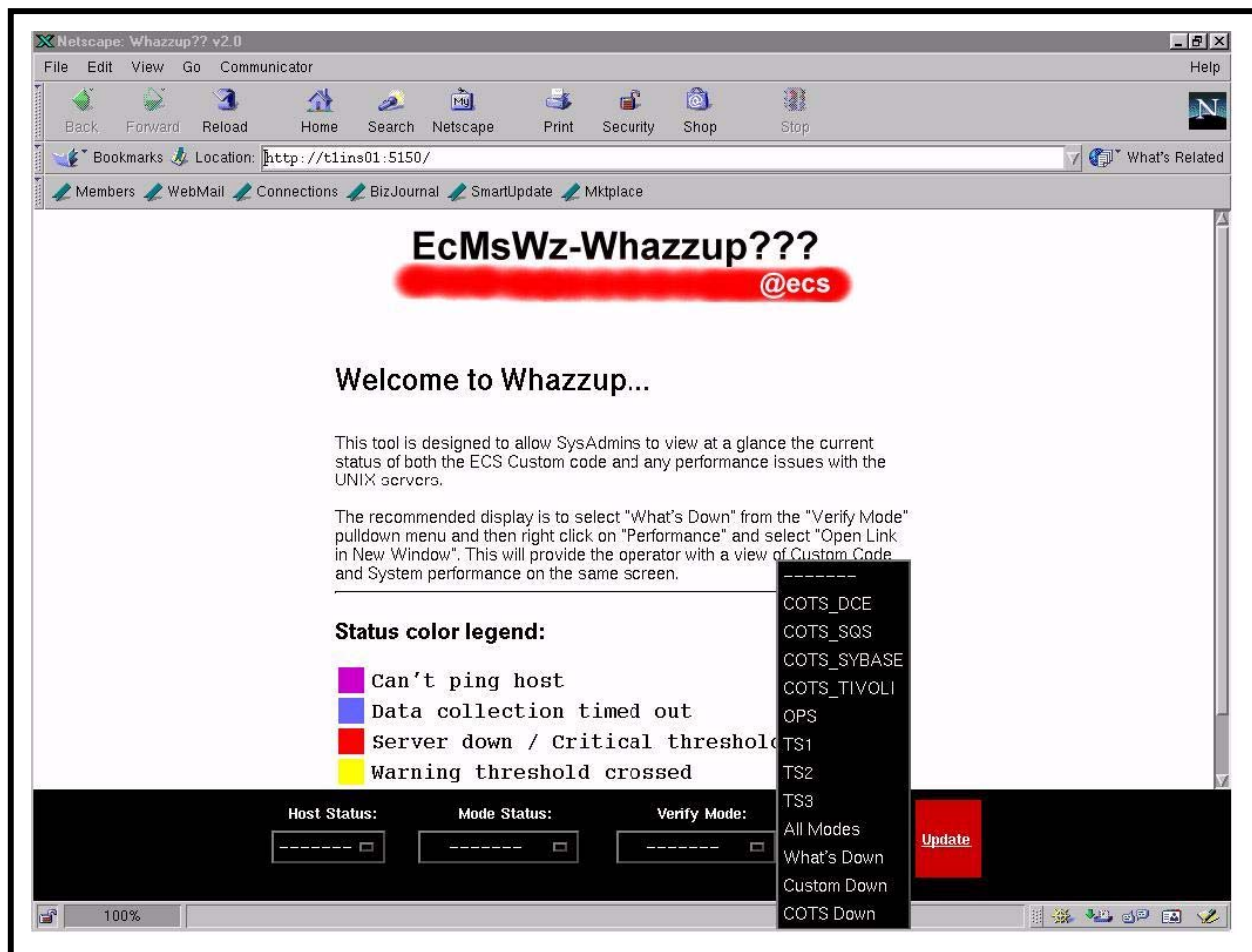
## Verify Mode

Selecting **Verify Mode** and choosing a desired mode (Figure 12) will provide a thorough display of ECS server status, by host, for the mode (Figure 13). Alternatively, selecting **What's Down** will provide a display indicating all down ECS servers, by mode, by host.

## Performance Management

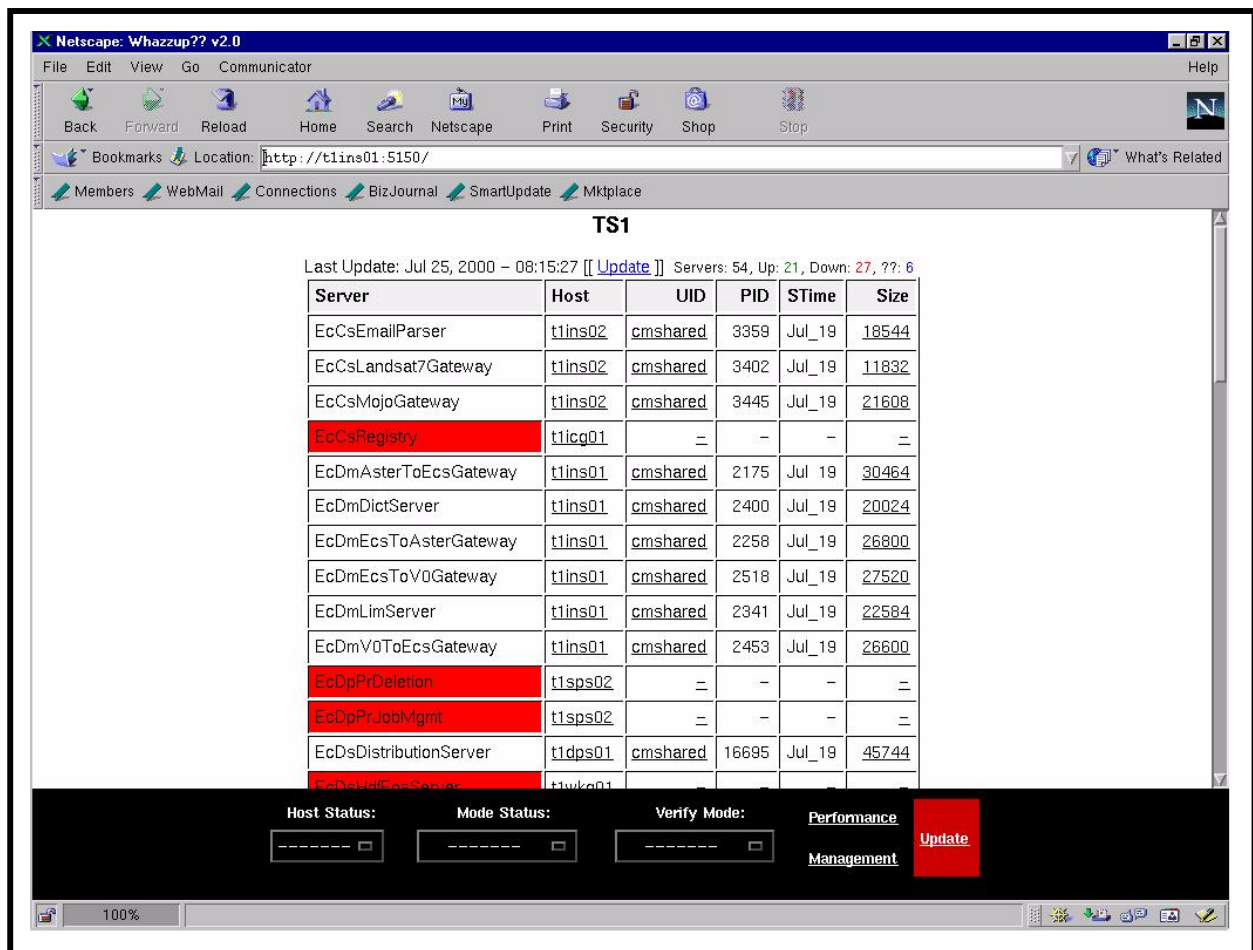
Following recommended monitoring procedures, the optimum method of system monitoring is to select **What's Down** from **Verify Mode** and then **Right Click** on **Performance Management** (Figure 14) and open the link in a new window (Figure 15).

Having these two displays active simultaneously will provide the Systems Administrator the status of "down" ECS servers and the performance status of individual hosts.

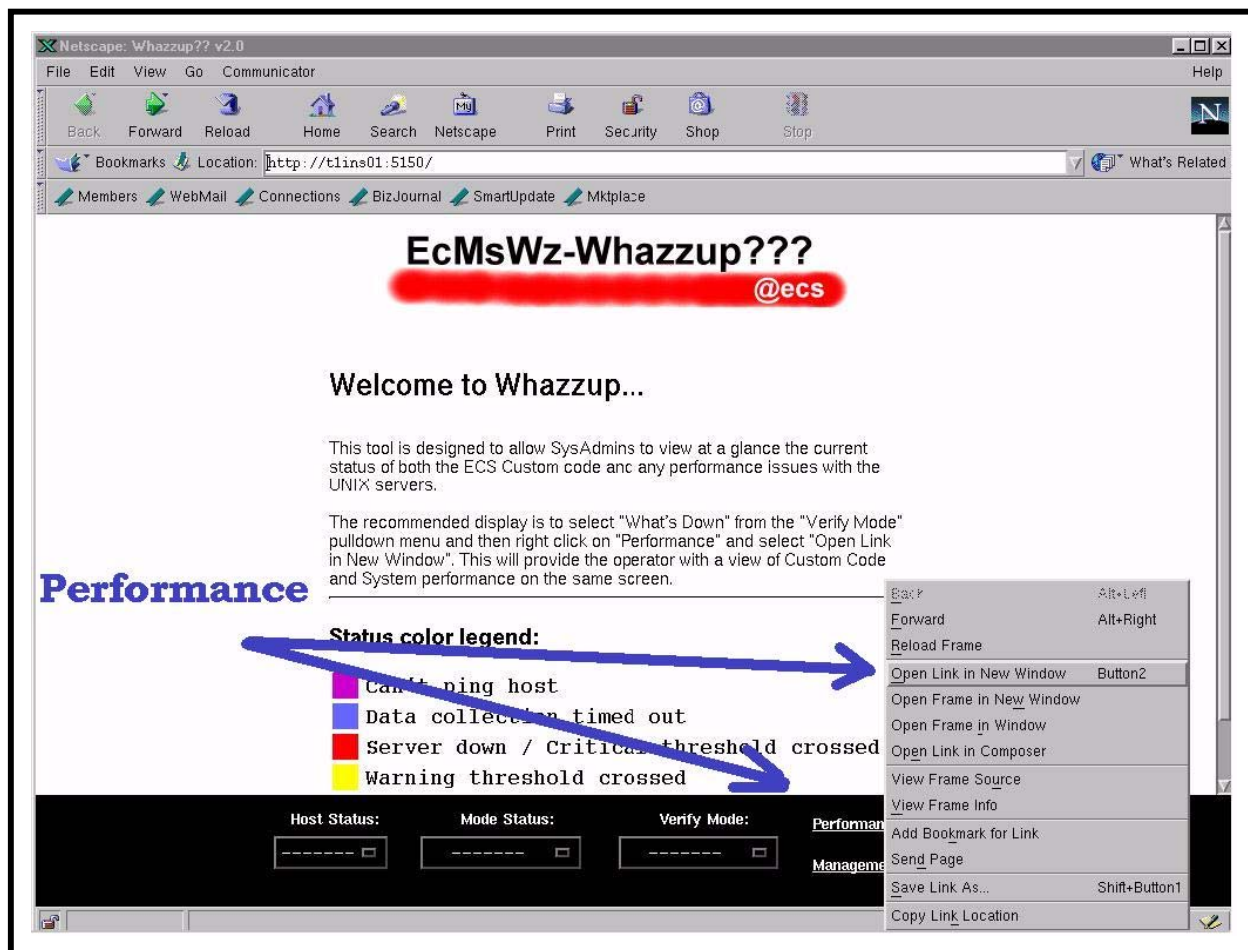


**Figure 12. Verify Mode Pop-Up Display**

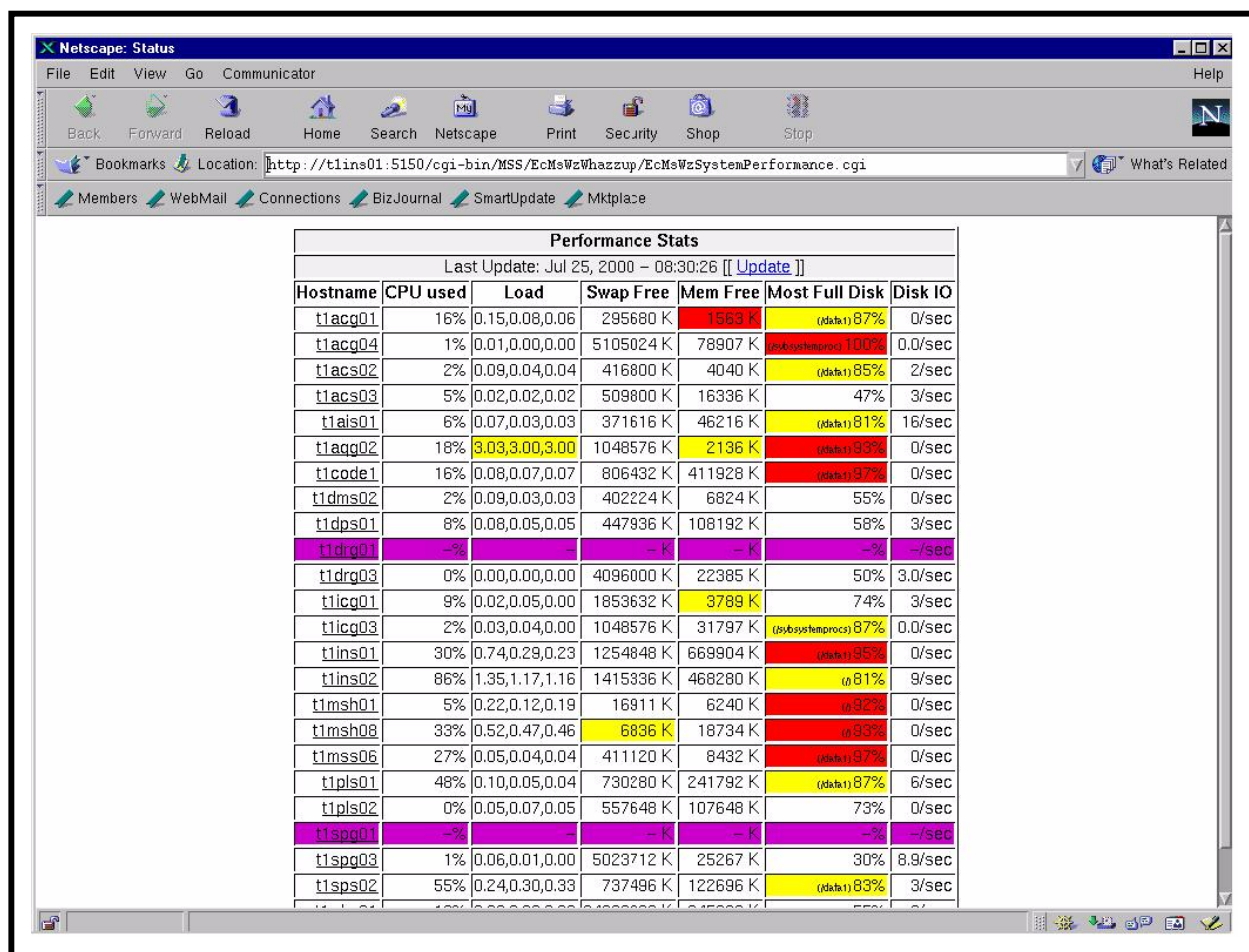




**Figure 13. Verify Mode Data Display**



**Figure 14. Performance Management Selection Display**



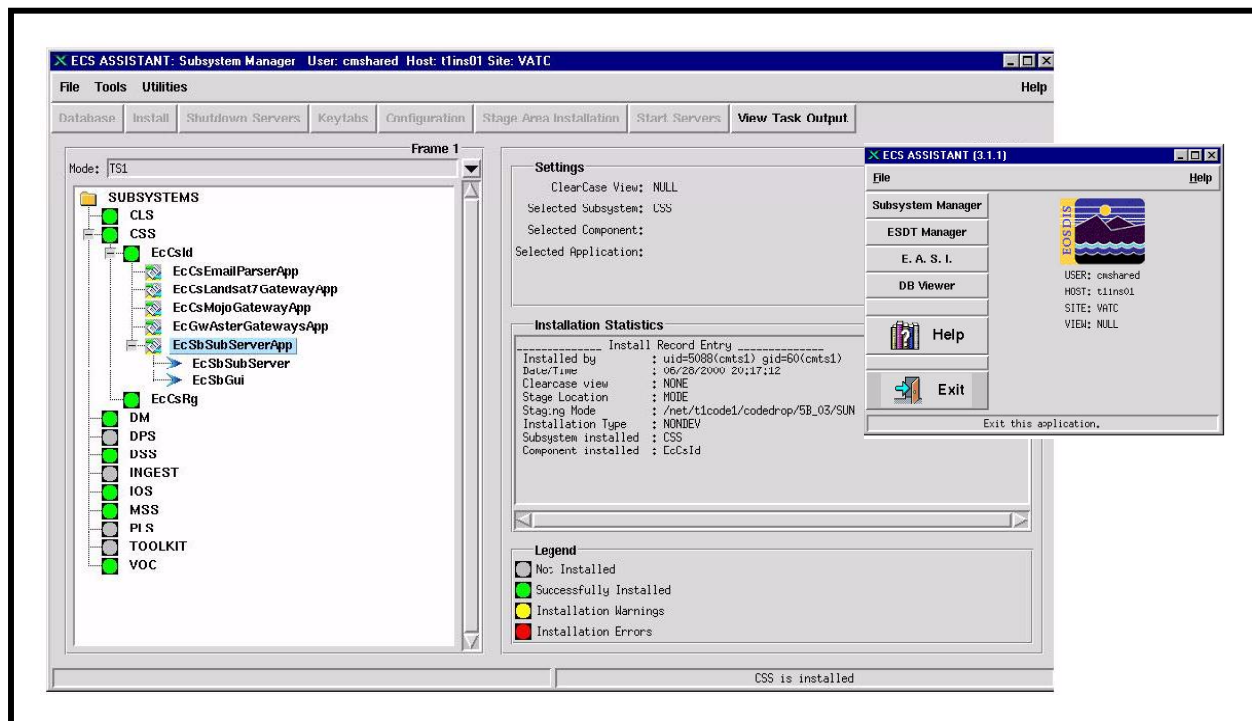
**Figure 15. Performance Management Data Display**

## ECS Assistant and ECS Monitor

The Whazzup tool provides a quick look capability to note whether any servers are down. The ECS Assistant and ECS Monitor tools provide additional easy-to-use tools that offer a server monitoring and ping capability (ECS Monitor) as well as a capability to start and stop servers (ECS Assistant). Figure 16 shows the ECS Assistant GUI for access to manager functions, the ECS Assistant subsystem manager GUI, and an example of a confirmation dialog.

### Starting ECS Assistant

- 1 Log in to one of the host machines.



**Figure 16. ECS Assistant GUI Manager Windows**

- 2 At the UNIX prompt on the host from which the ECS Assistant is to be run, type **setenv ECS\_HOME /usr/ecs** then press the **Return/Enter** key.
  - To verify the setting, type **echo \$ECS\_HOME** then press the **Return/Enter** key.
- 3 At the UNIX prompt, type **cd /tools/common/ea** then press the **Return/Enter** key. Then type **EcCoAssist /tools/common/ea &** then press the **Return/Enter** key.
  - **/tools/common/ea** is the path where ECS Assistant is installed, and also where EcCoScriptlib may be found.
  - The ECS Assistant GUI is displayed.
- 4 At the ECS Assistant GUI, click the **Subsystem Manager** pushbutton.
  - The Subsystem Manager GUI is displayed.
- 5 Select a mode by clicking on the down arrow at the right end of the **Mode** field and then on the desired mode name in the resulting list.
  - The selected mode is displayed in the **Mode** field and colored indicators show the installation status for components in that mode on the host; the legend for the color indications is at the lower right on the Subsystem Manager window.
- 6 In the list of subsystems, double click on the name of the subsystem of interest.
  - One or more component groups appear below the selected subsystem name.

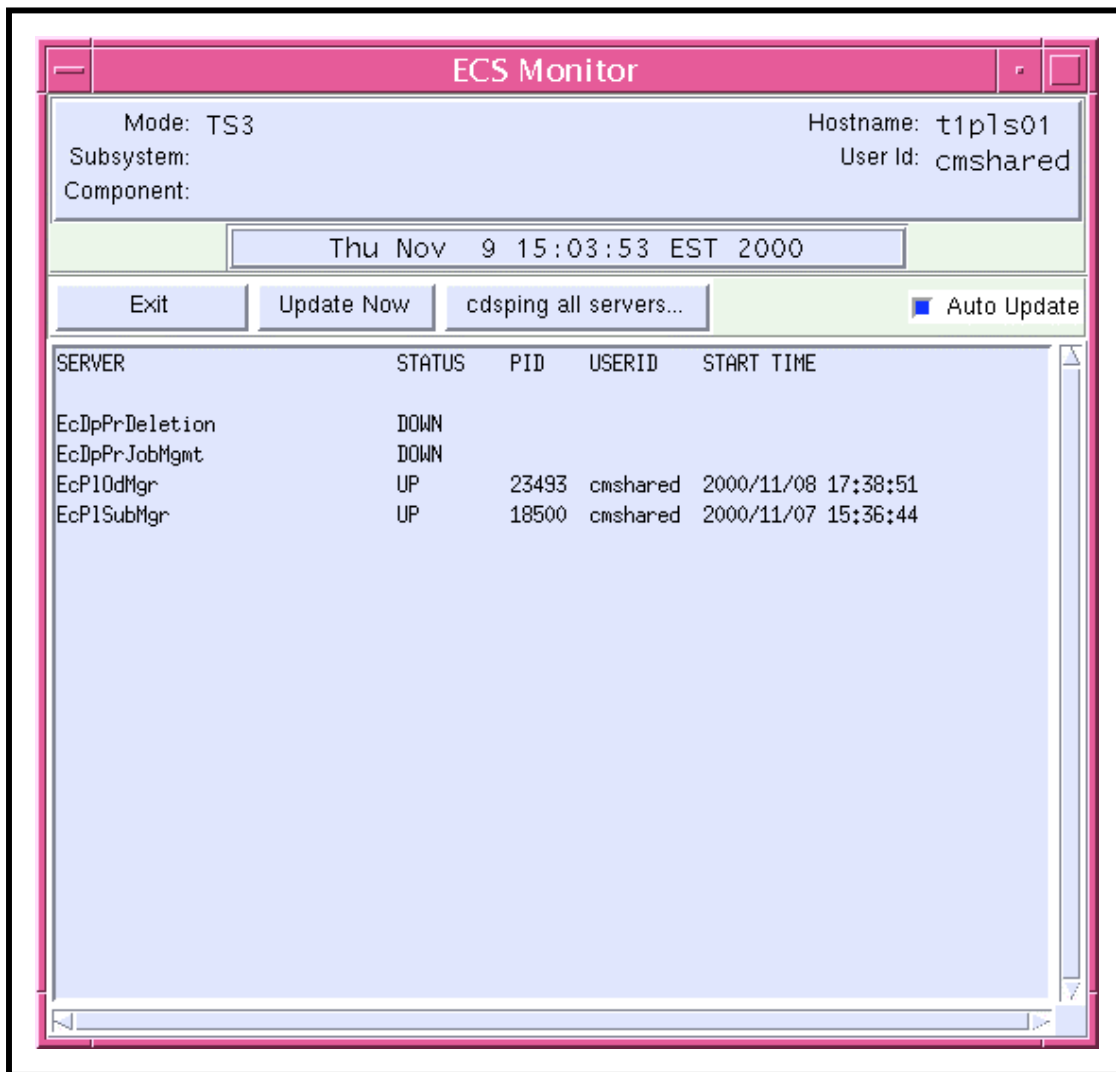
- 7 Double click on the name of a component group.
    - One or more application groups appear below the selected component group name.
  - 8 Double click on the name of the application group of interest.
    - The applications or servers in the selected group are listed below the name of the group.
  - 9 Single click on the name of an application or server of interest.
    - The selected application or server is highlighted.
    - Detailed installation information is displayed in the **Installation Statistics** window.
- 

ECS Monitor provides a convenient way to monitor the status of the servers by listing their up/down condition. The ECS Monitor GUI is shown in Figure 17; the status flag for a server is up or down indicating whether or not that server is running, and for a server that is running, the window shows the process ID (PID), the user ID, and the start time. There is a script that works with a *Sweeper* binary to ping the servers and clients in a mode to determine their status.

### Using the ECS Assistant Server Monitor

---

- 1 Log in to one of the host machines.
- 2 At the UNIX prompt on the host from which the ECS Assistant is to be run, type **setenv ECS\_HOME /usr/ecs** then press the **Return/Enter** key.
  - To verify the setting, type **echo \$ECS\_HOME** then press the **Return/Enter** key.
- 3 At the UNIX prompt, type **cd /tools/common/ea** then press the **Return/Enter** key.
  - **/tools/common/ea** is the path where ECS Monitor is installed.
- 4 Then type **EcCoMonitorGui /tools/common/ea <mode> &** then press the **Return/Enter** key.
  - **/tools/common/ea** is the path where EcCoScriptlib may be found.
  - The **ECS Monitor GUI** is displayed, showing the status (**UP** or **DOWN**) of the servers on the current host in the mode specified in the command, as indicated near the top left corner of the window.
  - The status “**UP/DOWN**” indicates whether a listed server is running.



**Figure 17. ECS Monitor GUI**

- 5 The **Server Monitor** GUI can be updated by clicking the **update** button in the GUI.
  - This causes the list to update to the current status.
- 6 To monitor other servers, log in to other hosts and launch the ECS Monitor GUI in the desired mode, as in Steps 2 through 4.
  - To exit, click the **EXIT** button. This terminates display of the monitor GUI.

---

Use the following procedure to ping servers.

## Using EcCsIdPingServers to Determine Server Status

---

- 1 Log in to one of the host machines.
- 2 At the UNIX prompt, type **cd /usr/ecs/<MODE>/CUSTOM/utilities** then press the **Return/Enter** key.
  - The prompt reflects a change to directory **cd /usr/ecs/<MODE>/CUSTOM/utilities**, where **<MODE>** is likely to be **OPS**, **TS1**, or **TS2**.
- 3 Then type **EcCsIdPingServers <MODE>** then press the **Return/Enter** key.

- The result should appear similar to the following:

```
/usr/ecs/DEV03/CUSTOM/bin/CSS/Sweeper -nsh dss2 -nsp 22822
FoSwSweeper application started...
We made a connection with EntryId =g0icg01:17871:12451240 ---
EcSrTransportEcInGranServer
We made a connection with EntryId =g0ins02:22336:6737528 --- DsHrQuitIDL
We made a connection with EntryId =g0pls02:35211:25637 --- PLOdMsgDObj
We made a connection with EntryId =g0dis02:48315:18311 ---
DsDdRequestMgrIDL
We made a connection with EntryId = g0ins02:17862:12461267 ---
InAutoIngestIF
We made a connection with EntryId = g0dis02:49473:13375 --- DsStReqMgrIDL
We made a connection with EntryId = g0ins02:41566:13071 --- IoAdRpc
We made a connection with EntryId = g0ins02:18139:12460808 ---
InRequestMgrIF
We made a connection with EntryId =g0dms03:42000:13266 ---
EcSrTransportDDICT
We made a connection with EntryId = g0pls02:22359:6737528 ---
    DsHrNonConfIDL681ab65e-60bc-1024-8e70-08006902a6d6
We made a connection with EntryId = g0pls02:22346:6737528 ---
    DsHrConformantIDL681ab65d-60bc-1024-8e70-08006902a6d6
We made a connection with EntryId =g0mss21:64657:8006 --- EcAcOrderMgr
We made a connection with EntryId =g0mss11:41449:22898 ---
EcSrTransportDarServer
We made a connection with EntryId = g0icg02:17724:12445092 --- EcRgRegistry
We made a connection with EntryId =g0mss11:41278:22739 ---
InDDNTransferPkt
We made a connection with EntryId =g0pls02:35085:25466 --- Deletion
We made a connection with EntryId =g0pls02:35168:25584 ---
SubscriptionQueue
We made a connection with EntryId =g0mss21:64700:8059 ---
MsAcUsrRequestMgr
We made a connection with EntryId =g0mss21:64690:8059 ---
```

**MsAcRegUserMgr**

**We made a connection with EntryId =g0mss21:64695:8059 ---**

**MsAcUsrProfileMgr**

**We made a connection with EntryId =g0pls02:35127:25527 ---**

**DpPrSchedulerDObj**

**We made a connection with EntryId =g0ins02:22364:6738409 ---**

**DsHrNonConfIDL681ab654-60bc-1024-8e70-08006902a6d6**

**We made a connection with EntryId =g0ins02:22353:6738409 ---**

**DsHrConformantIDL681ab653-60bc-1024-8e70-08006902a6d6**

**We made a connection with EntryId =g0ins02:22342:6738409 --- DsHrQuitIDL**

---



This page intentionally left blank.

# Tape Operations

---

In this lesson you will learn how Networker Administrative software and the Exabyte tape drive work together to administer the use of tapes for system backups and file restorations. Functions such as how to label a new tape, how to index a tape cartridge, and how to perform backups and restores are covered.

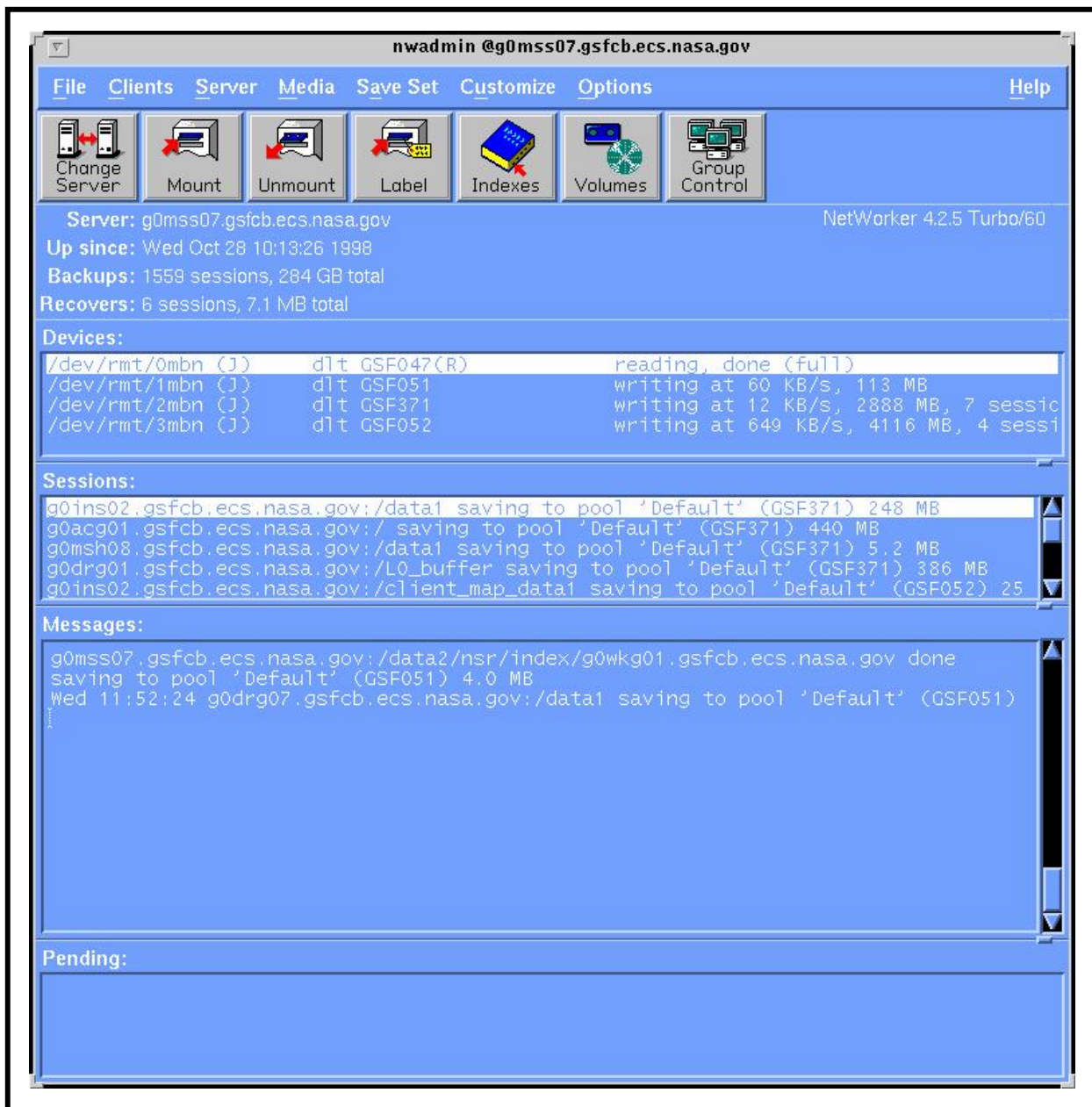
Terms:

- **Cartridge** - A hardware device that is part of the Exabyte tape drive. It holds up to 10 tapes that are automatically selected by Networker.
- **Drive** - Hardware device into which the tape or tape cartridge is inserted that performs the actual recording of data.
- **Index** - A list of the labeled tapes currently stored in the jukebox.
- **Inventory** - The action of making an index.
- **Jukebox** - A hardware device that stores more than one tape used for system backups and restores. Working in conjunction with specialized software, it can automatically select the proper tape, load the tape into the tape drive, and return it to its appropriate slot upon completion of the task.
- **Label** - A unique name assigned to a tape by Networker.
- **Volume** - A recording medium; in the case of this course, a volume and a tape are synonymous.

## Networker Administrator Screen

The main Networker Administrator screen (Figure 18), which is displayed after typing **nwadmin** at a UNIX prompt, contains four main sections:

- The menu bar at the top of the screen, which displays all of the possible capabilities of Networker Admin.
- The **speedbar**, which can be customized, displays icons that execute the most common procedures.
- Current configuration information, including the current Networker server, the available backup devices (tape drives, file systems, CD-ROMs, etc.).
- Current status windows, which display in real time the actual activity on the various devices, and progress and error messages.



**Figure 18. NetWorker Administrative Main Screen**

## Labeling Tapes

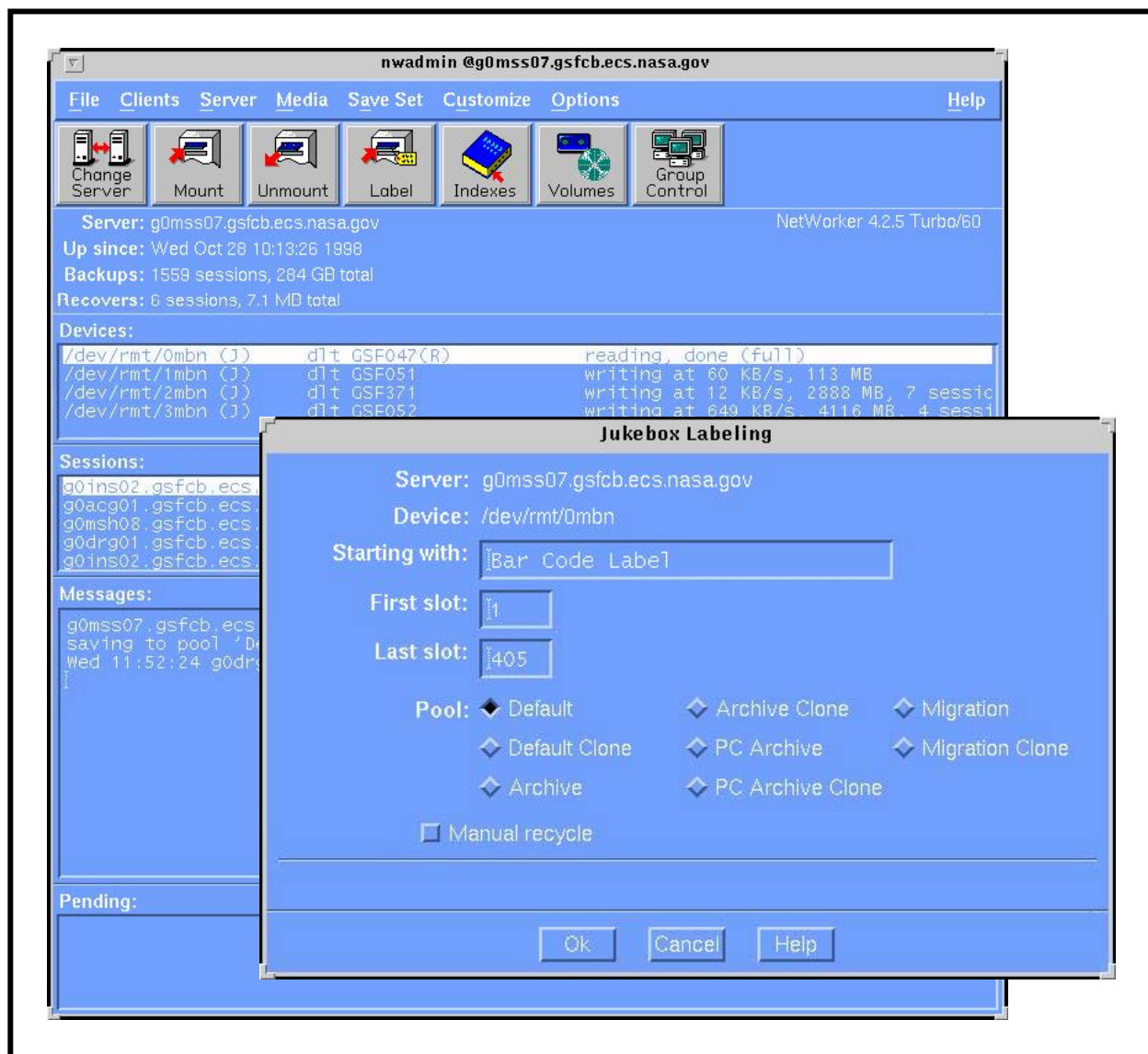
Files and directories have unique names that are assigned by the user to identify them. In much the same manner, tapes are given unique names, or labels. This allows such programs as NetWorker and such hardware devices such as the Exabyte jukebox to automate the tape selection process when performing system backups and restores. When a tape is initialized, NetWorker assigns it a label. NetWorker then stores the tape's label with a file that is written to

the tape so that when a file restoration request is received, Networker will know exactly which tape to select from the jukebox.

## Performing Tape Labeling

---

- 1 Login to a system terminal.
- 2 Set display to current terminal by typing: **setenv DISPLAY <IPNumber>:0.0** then press **Return/Enter**.
- 3 Start the log-in to the Backup client server by typing **/tools/bin/ssh BackupServerName** in the second window and then press the **Enter** key.
  - If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter passphrase for RSA key '<user@localhost>'** appears; continue with Step 3.
  - If you have not previously set up a secure shell passphrase, go to Step 4.
- 4 If a prompt to **Enter passphrase for RSA key '<user@localhost>'** appears, type your *Passphrase* and then press the **Enter** key. Go to Step 5.
- 5 At the **<user@remotehost>'s password:** prompt, type your *Password* and then press the **Enter** key.
- 6 Log in as root by typing: **su** then press **Return/Enter**.
  - A password prompt is displayed.
- 7 Enter the *RootPassword* then press **Return/Enter**.
  - Remember that *YourPassword* is case sensitive.
  - You are authenticated as yourself and returned to the UNIX prompt.
- 8 At the UNIX prompt, type **nwadmin** then press **Return/Enter**.
  - A window opens for the Networker Administrative program.
- 9 Insert the blank tape(s) in the jukebox's cartridge then install the cartridge in the jukebox.
  - Remove any non-blank tapes from the cartridge or else they will be re-labeled and the data on the tapes will be lost.
- 10 Click the **Label** button.
  - The **Jukebox Labeling** window opens (Figure 19).
- 11 In the field marked **Starting with**, enter the tape label you wish to use for the first tape in the sequence.
  - Tape labels are named by using the host name (e.g., **sprn1sgi**), a dot or period, and a sequential number (e.g., **001**, **002**).



**Figure 19. Jukebox Labeling Window**

- By default, the system will prompt you with the next label in the sequence (e.g., sprn1sgi.011).
- 12 In the **First Slot** field, enter **1** or the slot containing the first volume to be labeled; in the **Last Slot** field, enter **10** or the slot containing the last volume to be labeled.
- Slot 1 is at the top of the cartridge and 10 at the bottom.
  - Slot 11 is the non-removable slot within the jukebox. This usually contains a cleaning tape.
  - It is OK to leave empty slots.

- 13 Click the **OK** button.
    - A status message indicating the progress of the tape labeling procedure appears and updates.
    - Labeling a full cartridge of tapes takes about 15 minutes.
  - 14 When the status in the **Jukebox Labeling** window reads **finished**, click the **Cancel** button.
    - The **Jukebox Labeling** window closes.
  - 15 From the **File** menu, select **Exit**.
    - The **nwadmin** program terminates and you are returned to the UNIX prompt.
  - 16 At the UNIX prompt for the backup server, type **exit** then press **Return/Enter**.
    - **Root** is logged out.
  - 17 Type **exit** again then press **Return/Enter**.
    - You are logged out of and disconnected from the backup server.
  - 18 Put an identifying sticker on the outside of each tape cassette.
- 

## Indexing Tapes

Labeled tapes are loaded in a tape cartridge that is inserted into the Exabyte tape drive, also referred to as the jukebox. Networker needs to know the location of each tape in the jukebox. To do this, Networker uses a process called **inventory**, which prepares an index by matching a tape label to the cartridge slot that holds that tape (Figure 20). Then, when a request to recover a file or a set of files is received, *Networker* locates the tape based on the information in its memory.

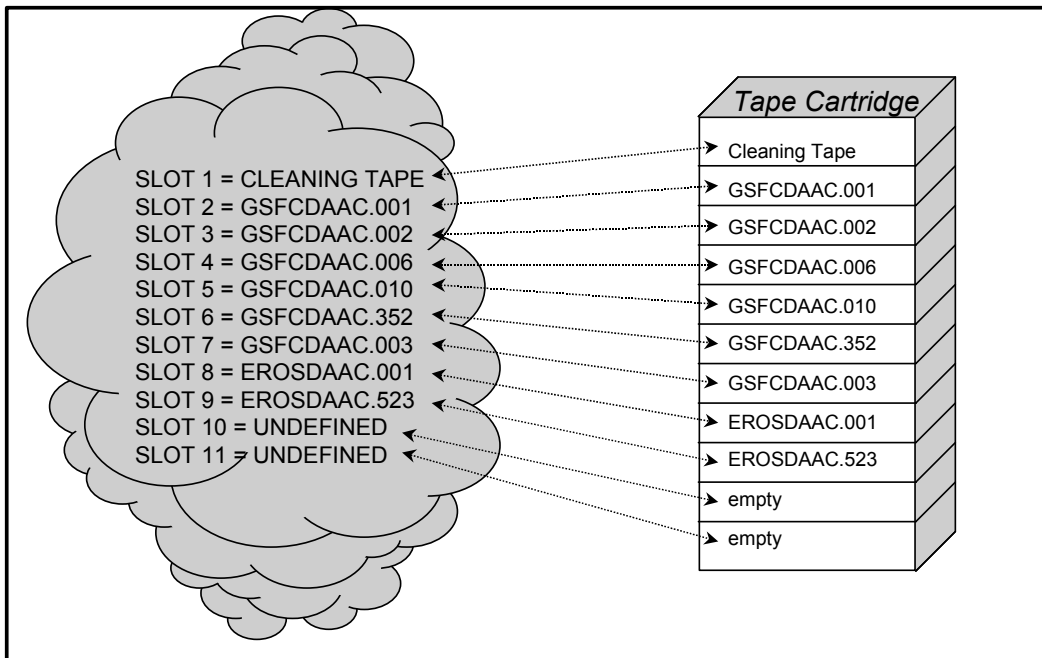
### CAUTION

*If you move a tape from its position in the cartridge, Networker will not know where to find it (Figure 21). You must re-index the cartridge by performing these procedures again for Networker to select the correct tape (Figure 22).*

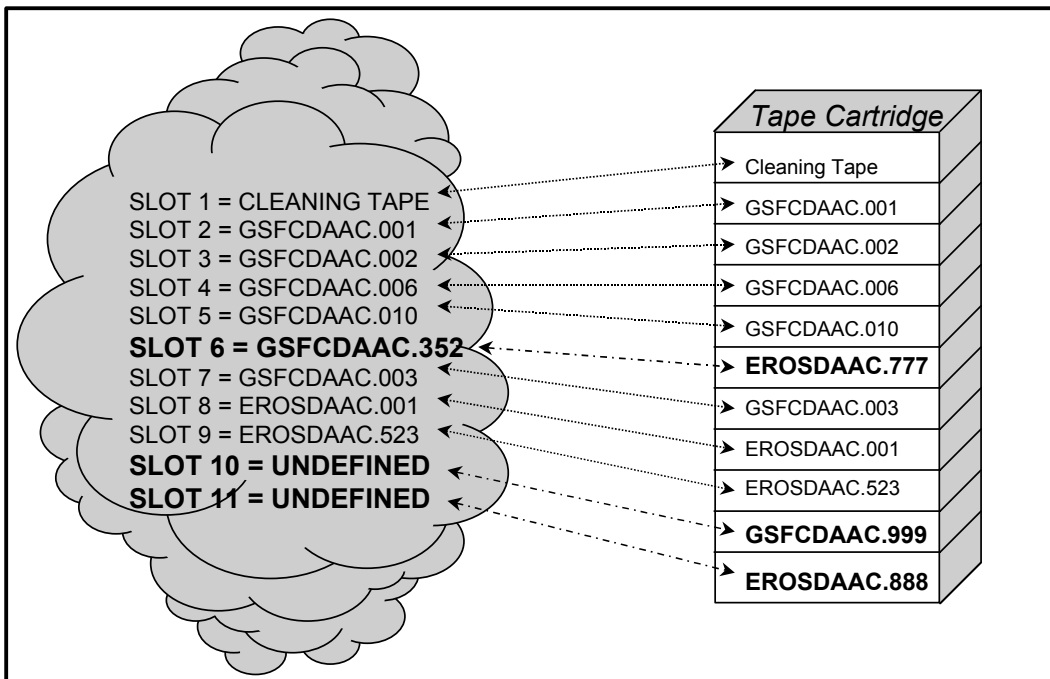
## Indexing Tape

---

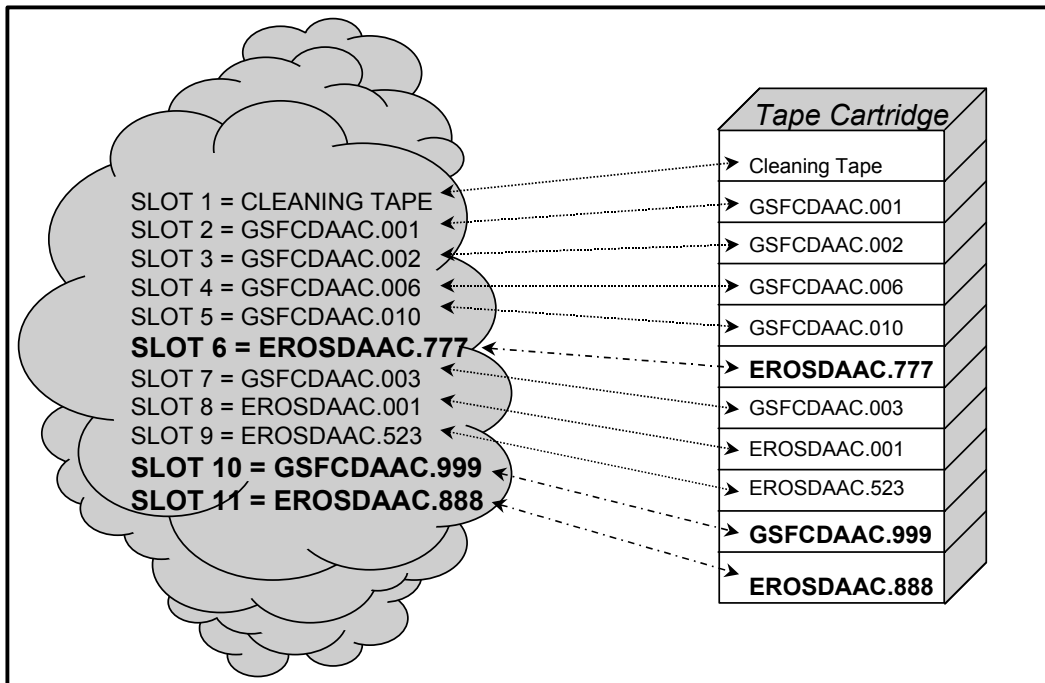
- 1 Login to a system terminal.
- 2 Set display to current terminal by typing: **setenv DISPLAY IPNumber:0.0** then press **Return/Enter**.



**Figure 20. Tape Index following the Initial Inventory**



**Figure 21. Tapes Changed but Not Re-Inventoried**

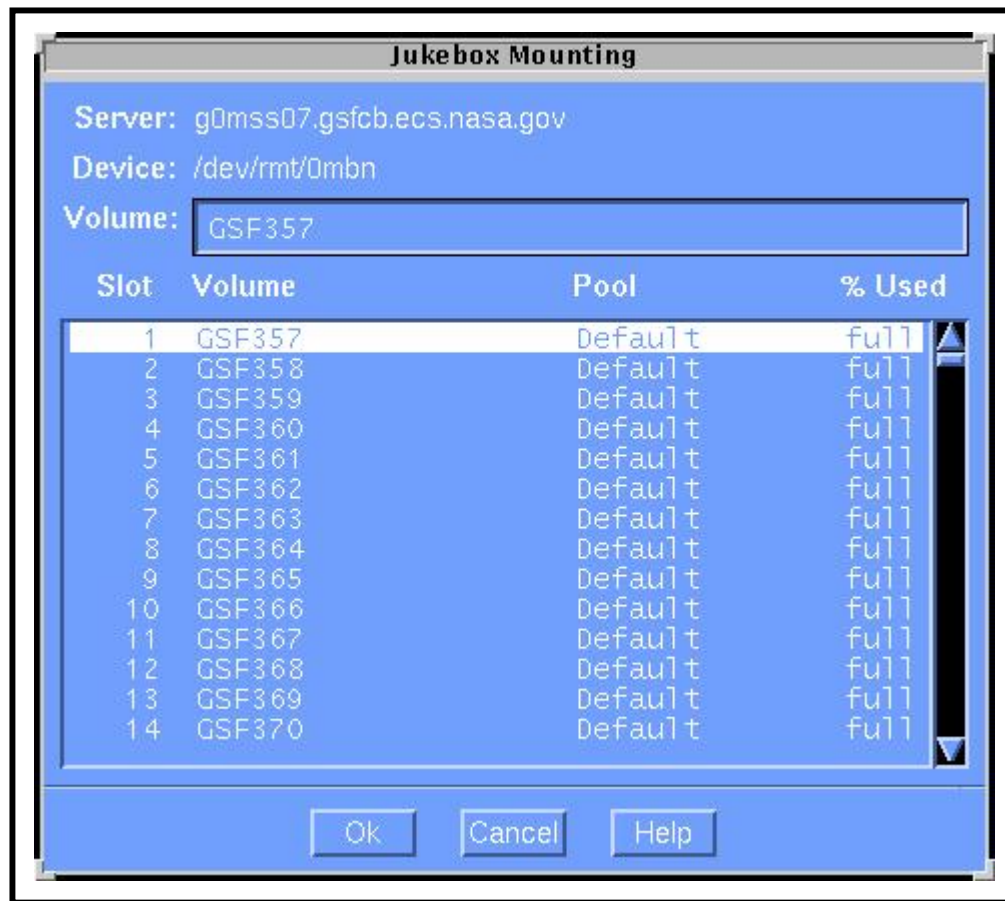


**Figure 22. Index is Updated after Re-Inventory**

- 3 Start the log-in to the Backup client server by typing **tools/bin/ssh BackupServerName** in the second window and then press the **Enter** key.
  - If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter passphrase for RSA key '<user@localhost>'** appears; continue with Step 3.
  - If you have not previously set up a secure shell passphrase, go to Step 4.
- 4 If a prompt to **Enter passphrase for RSA key '<user@localhost>'** appears, type your **Passphrase** and then press the **Enter** key. Go to Step 5.
- 5 At the **<user@remotehost>'s password:** prompt, type your **Password** and then press the **Enter** key.
- 6 Log in as root by typing **su** then press **Return/Enter**.
  - A password prompt is displayed.
- 7 Enter the **RootPassword** then press **Return/Enter**.
  - You are authenticated as root and returned to the UNIX prompt.
- 8 At the UNIX prompt, type **nwadmin** then press **Return/Enter**.
  - A window opens for the **Networker Administrative** program.



- 9 Click the **Mount** button, or select **Media -> Mount** from the menu.
- The **Jukebox Mounting** window opens (Figure 23) and displays a list of the tapes that Networker is currently aware of.
  - When you are finished with this window, click the **Cancel** button.



**Figure 23. Jukebox Mounting Window**

- 10 Insert the required tape(s) in the jukebox's cartridge then install the cartridge in the jukebox.
- Refer to the jukebox's documentation for detailed instructions on installing the cartridge.
- 11 Select **Media** from the menu bar then select **Inventory**.
- The **Jukebox Inventory** window opens.

- 12 In the **First Slot** field, enter **1** or the slot containing the first volume to be labeled; in the **Last Slot** field, enter **10** or the slot containing the last volume to be labeled.
    - Slot 1 is at the top of the cartridge and 10 at the bottom.
    - Slot 11 is the non-removable slot within the jukebox. This usually contains a cleaning tape.
    - It is OK to leave empty slots or slots with previously inventoried tapes.
  - 13 Click the **OK** button.
    - A status message indicating the progress of the tape indexing procedure appears and updates.
    - Inventorying a full cartridge of tapes takes between 20 and 30 minutes.
  - 14 When the **Jukebox Inventory** status reads **finished**, click the **Cancel** button.
  - 15 Click the **Mount** button to verify that the indexing worked.
    - The **Jukebox Mounting** window opens.
    - The **required tape(s)** should be shown. If not, repeat this procedure from Step 9.
  - 16 Click the **Cancel** button.
    - The **Jukebox Mounting** window closes.
  - 17 From the menu bar, select **File** then select **Exit**.
  - 18 At the UNIX prompt for the *BackupServer*, type **exit** then press **Return/Enter**.
  - 19 At the next UNIX prompt type **exit** again then press **Return/Enter**.
-

This page intentionally left blank.

# System Backups and Restores

---

Performing regular and comprehensive backups is one of the most important responsibilities a System Administrator has. Backups are the insurance that essentially all of the system data is always available. If the system crashes and all disks are damaged, the System Administrator should be able to restore the data from the backup tapes depending on backup method (e.g., full or partial).

## Incremental Backup

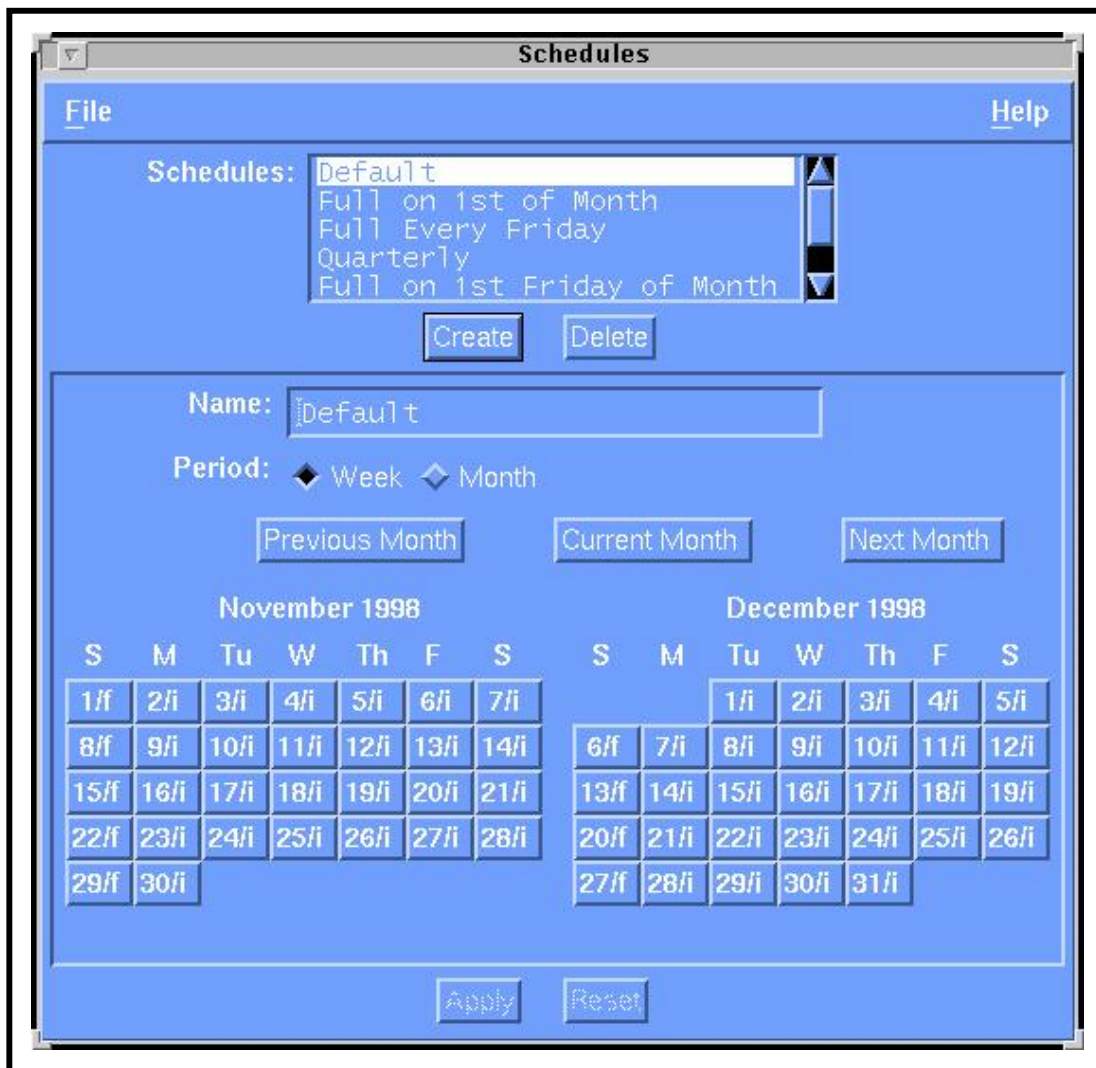
An incremental backup copies to tape all files on a system or subsystem that were created or modified since the previous incremental backup regardless of the backup level. The purpose of an incremental backup is to insure that the most recent edition of a file is readily available in case user error or disastrous system failure causes the file to become corrupt. Incremental backups are scheduled at a time that causes minimal disruption to the users. Copies of all incremental backup tapes are stored offsite for five weeks before they are reused.

Incremental backups are performed automatically according to the schedule setup in the Networker. Schedules windows (Figure 24). Incremental backups can also be requested at unscheduled times by completing the **Incremental Backup Request Form** and submitting it to the DAAC manager.

### Performing On-Demand Incremental Backup

---

- 1 Login to a system terminal.
- 2 Set display to current terminal by typing: **setenv DISPLAY IPNumber:0.0** then press **Return/Enter**.
- 3 Start the log-in to the Backup client server by typing **tools/bin/ssh BackedUpSystemName** in the second window and then press the **Enter** key.
  - If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter passphrase for RSA key '<user@localhost>'** appears; continue with Step 3.
  - If you have not previously set up a secure shell passphrase, go to Step 4.
- 4 If a prompt to **Enter passphrase for RSA key '<user@localhost>'** appears, type your **Passphrase** and then press the **Enter** key. Go to Step 5.
- 5 At the **<user@remotehost>'s password:** prompt, type your **Password** and then press the **Enter** key.



**Figure 24. Networker Schedules Window**

- 6 Log in as root by typing **su** then press **Return/Enter**.
  - A password prompt is displayed.
- 7 Enter the **RootPassword** then press **Return/Enter**.
  - You are authenticated as root and returned to the UNIX prompt.
- 8 At the UNIX prompt, type **nwadmin** then press **Return/Enter**.
  - A window opens for the Networker Administrative program.
- 9 Select **Customize → Schedules**.
  - The **Schedules** window opens.

- 10 Look at the button for today and note the letter on that day. If there is an **i** next to the date on this button, go to Step 11.
  - The **i** stands for incremental; **f** stands for full. Whichever is on the button for today is what kind of backup that will be done, unless it is overridden.
- 11 Click and hold the button for today, select **Overrides** from the resulting menu, select **Incremental** from the next resulting menu.
- 12 Click the **Apply** button.
- 13 Close the **Schedules** window by clicking in the upper left corner of the **Schedules** window and selecting **Close** from the resulting menu.
- 14 Click the **Group Control** button.
  - The **Group Control** window opens.
- 15 Click the **Start** button.
  - A **Notice** window opens.
- 16 Click the **OK** button.
  - The Notice window closes. The regularly scheduled backup will still run (even though we are now doing a backup).
- 17 Close the **Group Control** window by clicking in the upper left corner of the **Group Control** window and selecting **Close** from the resulting menu.
  - Status updates appear in the **nwadmin** window.
  - When the backup is complete, a **Finished** message will appear.
- 18 If the button for today in Step 10 had an **i** on it, go to Step 22.
- 19 Select **Customize → Schedules**.
  - The Schedules window opens.
- 20 Click and hold the button for today, select **Overrides** from the resulting menu, select **Full** from the next resulting menu.
- 21 Click the **Apply** button.
- 22 Close the **Schedules** window by clicking in the upper left corner of the **Schedules** window and selecting **Close** from the resulting menu.
- 23 Select **Exit** from the **File** menu to quit the Networker Administrative program.
  - The **nwadmin** window closes.
- 24 At the UNIX prompt for the machine to be backed up, type **exit** then press **Return/Enter**.
  - Root is logged out.

- 25     Type **exit** again then press **Return/Enter**.
- You are logged out and disconnected from the machine to be backed up.
- 

## Full System Backup

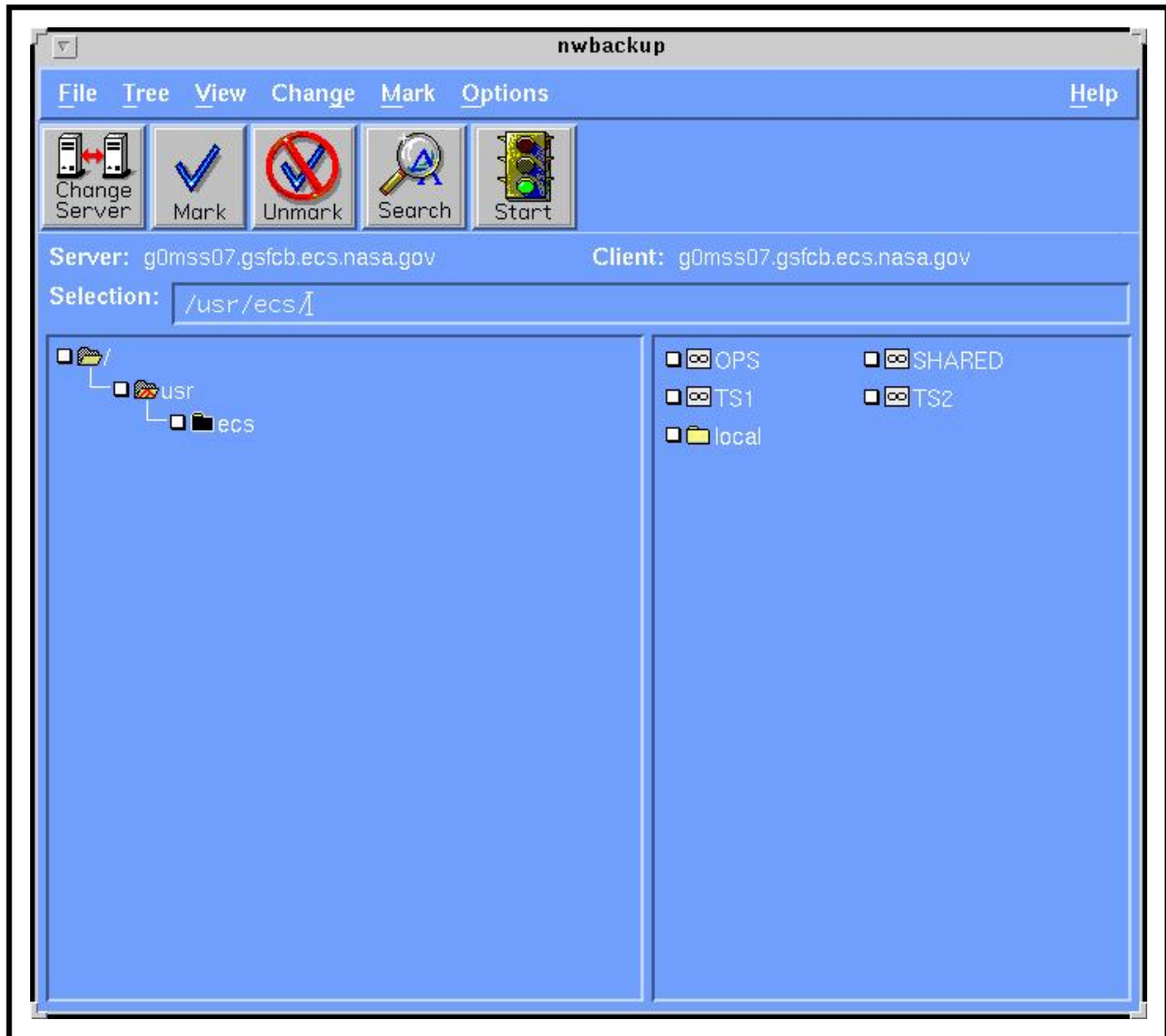
A full system backup is a snapshot of the data on the entire system as of a particular date. The data is stored on tapes that are used to recreate the system in the event of a total system failure. The full system backup is run by the System Administrator on a regular schedule, usually weekly. Full system backup tapes are stored offsite for security reasons.

### Performing Full Backup

---

- 1     Login to a system terminal.
- 2     Set display to current terminal by typing: **setenv DISPLAY IPNumber:0.0** then press **Return/Enter**.
- 3     Log **into** the machine to be backed up by typing: **/tools/bin/ssh BackedUpSystemName** then press **Return/Enter**.
  - If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter passphrase for RSA key '<user@localhost>'** appears; continue with Step 3.
  - If you have not previously set up a secure shell passphrase go to Step 4.
- 4     If a prompt to **Enter passphrase for RSA key '<user@localhost>'** appears, type your *Passphrase* and then press the **Enter** key. Go to Step 5.
- 5     At the **<user@remotehost>'s password:** prompt, type your *Password* and then press the **Enter** key.
- 6     Log in as root by typing **su** then press **Return/Enter**.
  - A password prompt is displayed.
- 7     **Enter** the *RootPassword* then press **Return/Enter**.
  - You are authenticated as root and returned to the UNIX prompt.
- 8     Execute the Networker Backup program by entering: **nwbackup** then press **Return/Enter**.

- A Networker Backup window opens (Figure 25). You are now able to perform a full backup.



**Figure 25. Networker Backup Window**

- 9 If no **files/directories to be backed up** were provided by the requester, i.e. the whole machine is to be backed up, then type / in the **Selection** field and click the **Mark** button.
  - / is designated for backup and has a check next to it.
- 10 If **files/directories to be backed up** were provided, then select the **files/directories to be backed up** in the directory display and click the **Mark** button.
  - Drag scroll bar with the mouse to scroll the list up and down.



- Double click on directory name to list its contents.
  - To move up a directory level, type the path in the **Selection** field.
  - Clicking the **Mark** button designates the file for backup and puts a check next to it.
- 11 Click the **Start** button.
- A **Backup Options** window opens.
- 12 Click the **OK** button.
- The **Backup Options** window closes.
  - The **Backup Status** window opens providing updates on the backup's progress.
- 13 After the **Backup Completion Time** message appears in the **Backup Status** window, click the **Cancel** button.
- The **Backup Status** window closes.
  - The backup is complete.
- 14 Select **Exit** from the **File** menu to quit the Networker Backup program.
- The Networker Backup window closes.
- 15 At the UNIX prompt for the **machine to be backed up**, type **exit** then press **Return/Enter**.
- Root is logged out.
- 16 Type **exit** again then press **Return/Enter**.
- You are logged out and disconnected from the machine to be backed up.
- 

## Single or Multiple File Restore

From time to time individual files or groups of files (but not all files) will have to be restored from an incremental backup tape due to operator error or system failure.

In order to perform the procedure, the System Administrator must have obtained the following information from the requester:

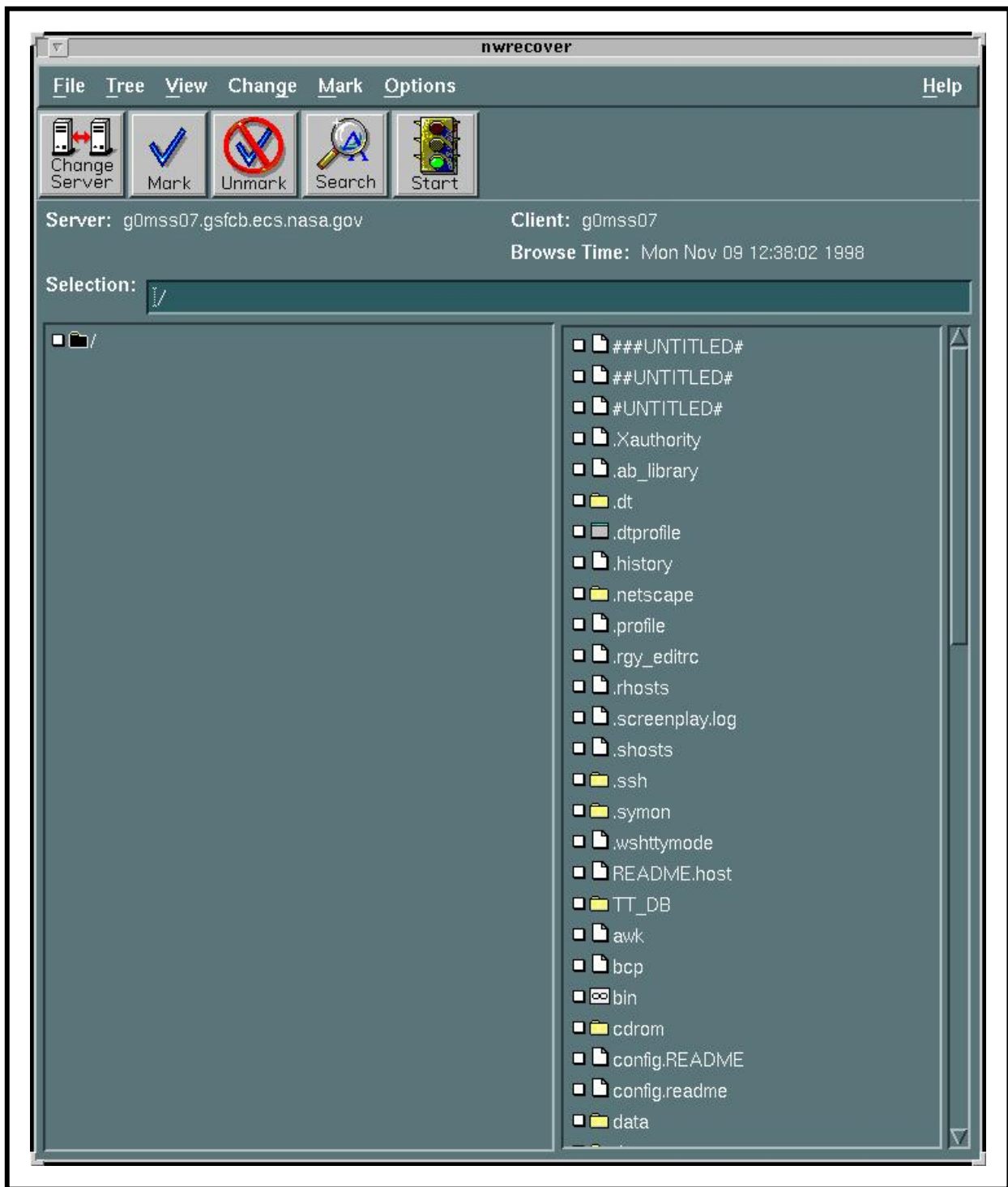
- Name of machine to be restored.
- Name of file(s) to be restored.
- Date from which to restore.
- User ID of the owner of the file(s) to be restored.

- Choice of action to take when conflicts occur. Choices are:
  - Rename current file
  - Keep current file
  - Write over current file with recovered file

## **Performing Single or Multiple File Restore**

---

- 1 Login to a system terminal.
- 2 Set display to current terminal by typing: **setenv DISPLAY IPNumber:0.0** then press **Return/Enter**.
- 3 Log into the machine to be restored by typing: **/tools/bin/ssh Machine Restored** then press **Return/Enter**.
  - If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter passphrase for RSA key '<user@localhost>'** appears; continue with Step 3.
  - If you have not previously set up a secure shell passphrase, go to Step 4.
- 4 If a prompt to **Enter passphrase for RSA key '<user@localhost>'** appears, type your **Passphrase** and then press the **Enter** key. Go to Step 5.
- 5 At the **<user@remotehost>'s password:** prompt, type your **Password** and then press the **Enter** key.
- 6 Log in as root by typing **su** then press **Return/Enter**.
  - A password prompt is displayed.
- 7 Enter the **RootPassword** then press **Return/Enter**.
  - You are authenticated as root and returned to the UNIX prompt.
- 8 Log in as the user by typing: **su User'sID**.
  - You are authenticated as the owner of the file(s) to be restored.
- 9 Execute the Networker Recovery program by entering: **nwrecover** then press **Return/Enter**.
  - A window opens for the **Networker Recovery** program (Figure 26). You are now able to restore files.



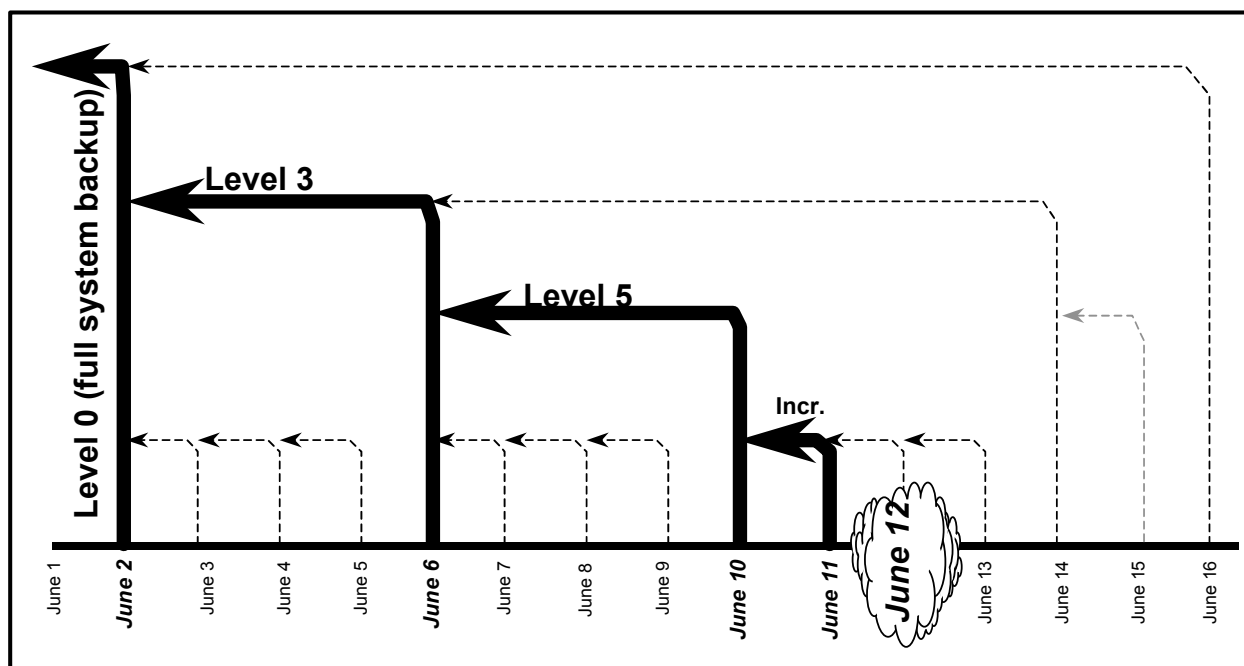
**Figure 26. Networker Recovery Window**

- 10 Select **file(s) to be restored** and click the **Mark** button.
    - Drag scroll bar with the mouse to scroll the list up and down.
    - Double click on directory name to list its contents.
    - Clicking the **Mark** button designates the file for restore and puts a check next to it.
  - 11 Select **Change → Browse Time**.
    - The **Change Browse Time** window opens.
  - 12 Select the **date from which to restore**.
    - Networker will automatically go to that day's or a previous day's backup which contains the file.
  - 13 Click the **Start** button.
    - The **Conflict Resolution** window opens.
  - 14 Answer "Do you want to be consulted for conflicts" by clicking the **yes** button, then click the **OK** button.
    - If prompted with a conflict, choices of action will be: rename current file, keep current file, or write over current file with recovered file.
    - Select the requester's **choice of action to take when conflicts occur**.
    - The **Recover Status** window opens providing information about the to be restored.
    - If all the required tapes are not in the drive, a notice will appear.
    - Click the **OK button** in the notice window.
  - 15 When a **recovery complete** message appears, click the **Cancel** button.
  - 16 Select **File → Exit**.
    - The Networker Recovery program quits.
  - 17 Type **exit** then press **Return/Enter**.
    - The owner of the file(s) to be restored is logged out.
  - 18 Type **exit** again then press **Return/Enter**.
    - Root is logged out
  - 19 Type **exit** one last time then press **Return/Enter**.
    - You are logged out and disconnected from the **machine to be restored**.
-

## Complete System Restore

A complete system restore is an emergency procedure that should be performed only in the event of a system crash with the loss of data. The only way to get the system back up and running in a timely fashion is to restore the system from a previous backup. The result of this action will be that any updates to the system between the last backup and the time of the restore will be lost. The System Administrator will determine which complete backup tape(s) to use (Figure 27). Depending on the frequency of complete system backups and incremental backups, data loss can be minimized.

A complete system restore involves restoring a number of tapes depending upon the particular situation. For example, should a system failure occur immediately after a full system backup was performed, only the tapes used in that backup will be required to restore the system to its usable state. However, if there was a period of time between the last full system backup and the system failure, tapes from the last full system backup as well as partial and incremental backups will have to be restored. This may become a time consuming process depending on the server affected, how much data is to be recovered, and how many tapes need to be restored. Additionally, the System Administrator may determine that only one or two of the many partitions need to be restored to make the system whole again. Therefore, these procedures will have to be mixed and matched to determine the proper restoration procedure for a given situation.



**Figure 27. Tapes Required for Full System Restore**

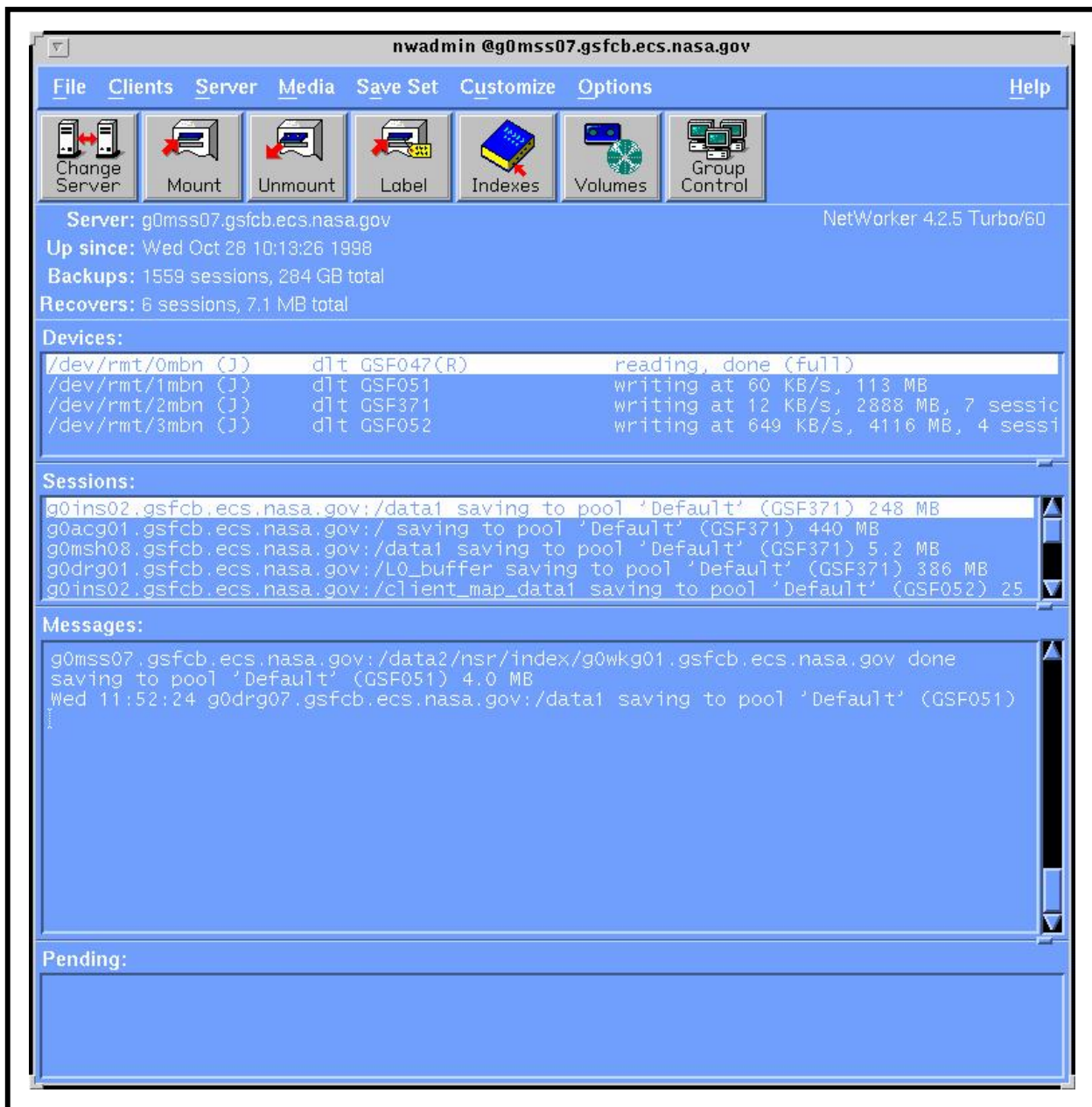
To perform the procedure, the SA must have the following information about the requester:

- Name of system to be restored
- Date from which to restore

### Performing Full System Restore

---

- 1 Log into the backup server by typing: **/tools/bin/ssh *BackupServerName*** then press **Return/Enter**.
- 2 Set display to current terminal by typing: **setenv DISPLAY *IPNumber:0.0*** then press **Return/Enter**.
- 3 Log into the machine to be restored by typing: **/tools/bin/ssh *Machine Restored*** then press **Return/Enter**.
  - If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter passphrase for RSA key '<user@localhost>'** appears; continue with Step 3.
  - If you have not previously set up a secure shell passphrase, go to Step 4.
- 4 If a prompt to **Enter passphrase for RSA key '<user@localhost>'** appears, type your **Passphrase** and then press the **Enter** key. Go to Step 5.
- 5 At the **<user@remotehost>'s password:** prompt, type your **Password** and then press the **Enter** key.
- 6 Log in as root by typing **su** then press **Return/Enter**.
  - A password prompt is displayed.
- 7 Enter the **RootPassword** then press **Return/Enter**.
  - You are authenticated as root and returned to the UNIX prompt.
- 8 Set display to current terminal by typing: **setenv DISPLAY *IPNumber:0.0*** or **setenv DISPLAY *BackupServerName:0.0*** then press **Return/Enter**.
- 9 Log in as the user by typing: **su *User'sID***.
  - You are authenticated as the owner of the file(s) to be restored.
- 10 Set display to current terminal by typing: **setenv DISPLAY *IPNumber:0.0*** or **setenv DISPLAY *MachineRestored:0.0*** then press **Return/Enter**.
- 11 Execute the Networker Administrator program by entering: **nwadmin** then press **Return/Enter**.
  - A window opens for the Networker Administrator program (Figure 28).
  - You are now able to perform restores of partitions.



**Figure 28. NetWorker Administrator's Window**

- 12 Select **Save Set** → **Recover Set**.
  - The **Save Set Recover** window opens.
- 13 Select the **Name of system to be restored** (referred to as **System** in the rest of this procedure) in the **Client** field's menu.
  - The **Save Set** listing updates. This is a listing of partitions on the **System**.

- At this time, note the partitions listed for the **System**. To do a complete system restore, this procedure needs to be performed for each partition listed.
- 14** Select the **Save Set**/partition from the listing.
- The **Instance** listing updates.
- 15** Select the appropriate **Instance**.
- An **Instance** is a particular Networker client backup. A listing of **Instances** is a report detailing the Networker client backups that have occurred.
  - Select an **Instance** based upon the **Date from which to restore** (referred to as **Date** in the rest of this procedure) and of an appropriate level:
    - To determine a base **Date**, you must consider the time of day that backups occur. For example, if the backup occurs at 02:00 each morning then a system corrupted at noon on June 6 would require a restoration of the June 6 backup. However, if the system corruption took place around the time of the backup, it would be more prudent to use the backup from June 5.
  - If the backups are full or incremental, perform the following actions:
    - Select the most recent full backup that occurred on or prior to the **Date** and perform a partition restore. If the date of this full backup is not the same as the **Date**, perform a partition restore using each incremental backup, in chronological order, between this full backup and the day after the **Date**.
  - If the backups are of different numerical levels, follow these steps:
    - First select the most recent level 0/full backup prior to or on the **Date** and perform a restore of the partition. If a level 0/full backup did not occur on the **Date**, select the most recent backup of the next highest level occurring after this level 0 and prior to or on the **Date**.
    - Perform a restore of the partition. Continue to select the most recent backup of the next highest level occurring between the last used **Instance** and the day after the **Date** until reaching an instance on the **Date**.
  - You can double click an **Instance** to see which tape is required.
- 16** Click the **Recover** button.
- The Save Set Recover Status window opens.
  - Clicking the Volumes button will show which tapes are required.
- 17** Click the **Options** button.
- The Save Set Recover Options window opens.
- 18** Set Duplicate file resolution to Overwrite the existing file by clicking its radio button.



- 19 Make sure that the **Always prompt** checkbox is not checked.
  - 20 Click the **OK** button.
    - The **Save Set Recover Options** window closes.
  - 21 Click the **Start** button in the **Save Set Recover Status** window.
    - Status messages appear in the **Status** box.
    - A **recovery complete** message appears when recovery is complete.
  - 22 Click the **Cancel** button after the **recovery complete** message appears.
    - The **Save Set Recover Status** window closes.
  - 23 If additional partition restores are required, go to Step 12. Otherwise, select **Exit** from the **File** menu to quit the Networker Administrator program.
  - 24 At the UNIX prompt for the backup server, type **exit** then press **Return/Enter**.
  - 25 Type **exit** again then press **Return/Enter**.
-

# User Administration

---

## Screening Personnel

### Screening Criteria

Some positions require special access privileges in order to do the assigned job or duties. These are called public trust positions because they can affect the integrity, efficiency, or effectiveness of the system to which they have been granted privileged access. Screening for suitability, prior to being granted access, is required. This screening, National Agency Check (NAC), is required to ensure that granting any special access privileges to someone would not cause undue risk to the system for which that employee has these privileges. Line Management is responsible for requesting suitability screening for the employees in their respective organizations.

OMB Circular A-130, Appendix III and NPR 2810.1 require the following employees to undergo personnel screening:

- All employees who require privileged access or limited privileged access to a Federal computer system or network.
- Privileged access – Can bypass, modify, or disable the technical or operational system security controls.
- Limited privileged access – Can bypass, modify or disable security controls for part of a system or application but not the entire system or application.

Internet Protocol Operational Network (IONet) Access Protection Policy and Requirements (290-004) requires the following employees to undergo suitability screening:

- All employees who require privileged access, limited privileged access, or access to the Closed Segment of the Internet Protocol Operational Network (IONet) (formerly NASCOM).
- All employees having access to IONet network control devices.

NPR 1620.1A requires that all employees granted unescorted access to a NASA Resource Protection (NRP) facility or area and/or a NASA-designated Limited Area undergo screening.

### Screening Procedures

The line manager will submit NASA Form 531 containing the following information for each employee needing suitability screening.

- Full name (first, middle initial and last)
- Goddard badge number if badged employee

- Reason for requesting screening
- Type and date of any previous security investigation or clearance if known
- Phone number and email address

The request should be sent to the EDF Security Administrator. The GSFC Security Office (GSO) will search the personnel security database to determine if a current NAC has been performed. If not the employee will be contacted to obtain additional information. The GSO will report a favorable or unfavorable result back to the EDF Security Administrator upon completion of the suitability screening.

## Adding a New User

Adding a user to the system is accomplished through a series of steps that may be performed as a suite from the command line or by use of a script. The procedure below outlines the individual steps that are required to completely set up a new user on the system. The scripts will accomplish these steps in an interactive manner.

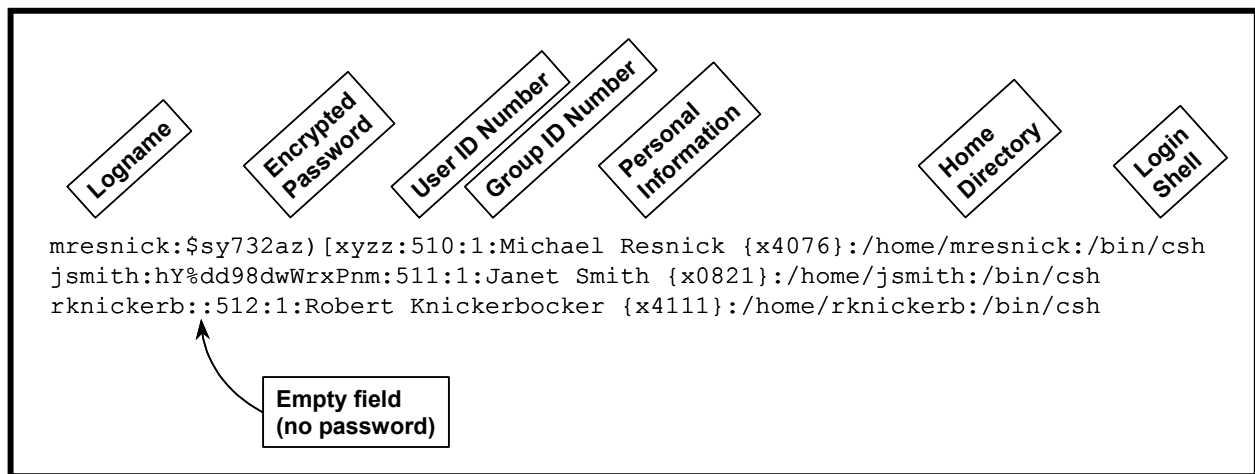
The requester fills out a User Registration Request Form and submits it to the requestor's supervisor. The requester's supervisor reviews the request, and if s/he determines that it is appropriate for the requester to have an account, forwards the request to the System Administrator. If the requester requires a National Agency Check (NAC) before access is granted, the supervisor will forward the request to the Security System Engineer, who will then ensure that proper procedures are followed before the request is sent to the System Administrator (SA). The System Administrator verifies that all required information is contained on the form. If it is, s/he forwards the request to the approval authority, the DAAC Manager. Incomplete forms are returned to the requester's supervisor for additional information. If the request for the accounts fits within policy guidelines, the DAAC Manager approves the request and returns the request form to the System Administrator to implement.

The System Administrator should be familiar with a UNIX text editor and the files **/etc/passwd.y** (Figure 29), **/etc/group** (Figure 30), and **/etc/auto.home**.

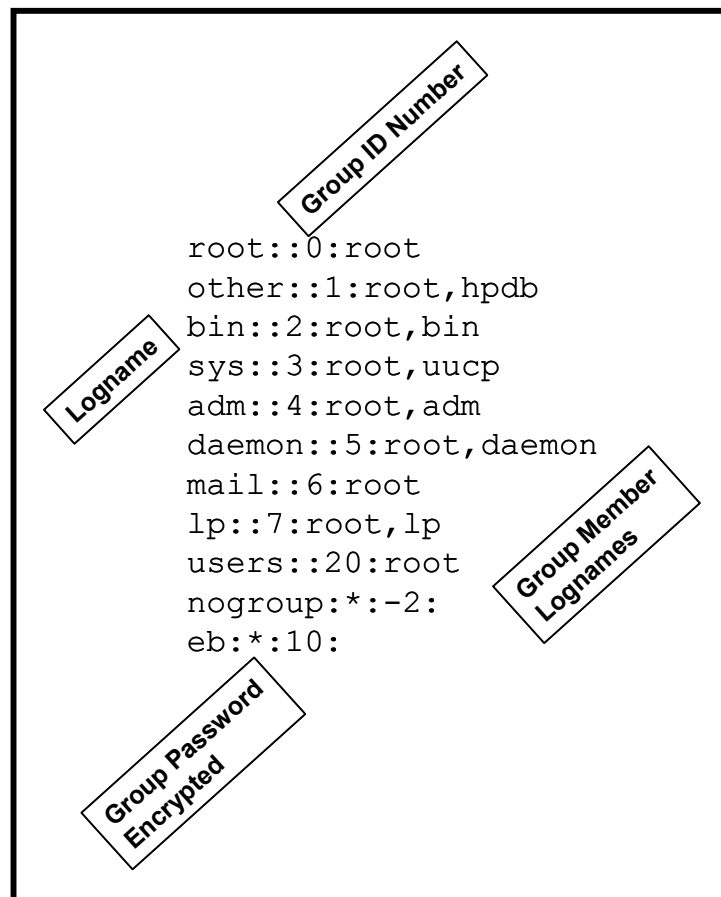
The System Administrator (SA) creates a new user account with command-line/script entries. As an example, The Goddard Space Flight Center DAAC uses a script, *Newuser*, to add new users to the system. The script, which is available to other DAACs, walks the System Administrator through data input of user information, checks for the same user in other systems, creates a User ID, synchronizes password files and creates home directories for new users.

## Deleting a User

The Deleting a User process begins when the requester has determined that no useful files remain in the user's home directory and submits a request to delete the user's account to his/her supervisor. The supervisor approves or denies the request. Once approved, the request is forwarded to the OPS Super. The OPS Super reviews the request and forwards it to the SA who deletes the user's account. When the user has been deleted, the SA notifies the requester, supervisor and OPS Super.



**Figure 29. `/etc/passwd` File Fields**



**Figure 30. `/etc/group` File**

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that the requester's application for deleting a user has already been approved by DAAC Management. In order to perform the procedure, the SA must have obtained the following information from the requester:

- **UNIX login of the user to be deleted**
- **Role(s) of the user to be deleted**

The System Administrator deletes a user with command-line/script entries. As an example, The Goddard Space Flight Center DAAC uses a script, *Lockdown*, to lock, unlock and delete user accounts. This script, which is available to other DAACs, walks the System Administrator through the steps necessary to delete a user account. It assists the System Administrator in locating the correct user account for deletion and deletes the user account and all associated file references. It also enables the System Administrator to lock or unlock accounts.

## **Changing a User's Account Configuration**

Account configuration is accomplished through command line and script. The DAAC manager must authorize changes to user accounts.

The Changing a User Account Configuration process begins when the requester submits a request to the OPS Super detailing what to change about the account configuration and the reason for the change. Requests for changes to privileged accounts shall be sent to the Security System Engineer. The OPS Supervisor or the Security System Engineer reviews the request and forwards it to SA who changes the user's account configuration. When the changes are complete the SA notifies the requester and OPS Supervisor.

In order to perform the procedure, the System Administrator must have obtained the following information from the requester:

- What to change and new settings. Can be any of:
  - New Real User Name
  - New Office Number
  - New Office Phone Number
  - New Home Phone Number
  - New UNIX Group
  - New Login Shell
- Current UNIX Login of the User

## **Changing User Access Privileges**

The Changing User Access Privileges process begins when the requester submits a request to his/her supervisor. Requests for changes to privileged accounts shall be sent to the Security

System Engineer. The supervisor or the Security System Engineer approves or denies the request. Once approved, the request is forwarded to the OPS Super. The Ops Super reviews the request and forwards it to the SA who changes the user's access privileges. When the changes are complete the SA notifies the requester, supervisor and Ops Super.

In order to perform the procedure, the System Administrator must have obtained the following information about the requester:

- Role(s) to which the user is to be added
- Role(s) from which the user is to be removed
- UNIX login of the user

## Changing a User Password

The Changing a Users Password process begins when the requester submits a request to the SA. The System Administrator verifies that the requester is who s/he claims to be. Once verified, the SA changes the user's password. When the change is complete the SA notifies the requester.

Detailed procedures for tasks performed by the SA are provided in the sections that follow.

The procedures assume that the requester's application for changing a user password has already been approved by DAAC Management. In order to perform the procedure, the SA must have obtained the following information about the requester:

- UNIX login of the user
- New password for the user

To change a user password for the requester, execute the command line or script procedure steps that have been developed.

## Checking a File/Directory Access Privilege Status

### Checking File/Directory Access Privileges

---

- 1 At a UNIX prompt, type **cd *Path*** then press **Return/Enter**.
  - The ***Path*** is the full path up to but not including the file/directory on which access privilege status is needed. For example, if the requester wants access privileges status on directory /home/jdoe, type **cd /home** then press **Return/Enter**.
- 2 From the UNIX prompt, type **ls -la**. The output from the command should appear as below:

drwxrwxrwx	3	mresnick	training	8192	Jun 14 08:34	archive
drwxr-xr-x	11	mresnick	training	4096	Jul 03 12:42	daacdata
-rw-rw-rw-	1	mresnick	training	251	Jan 02 1996	garbage
lrw-r--r--	2	jjones	admin	15237	Apr 30 20:07	junk

-rwxr--rw-	1	mresnick	training	5103	Oct 22 1994	trash
------------	---	----------	----------	------	-------------	-------

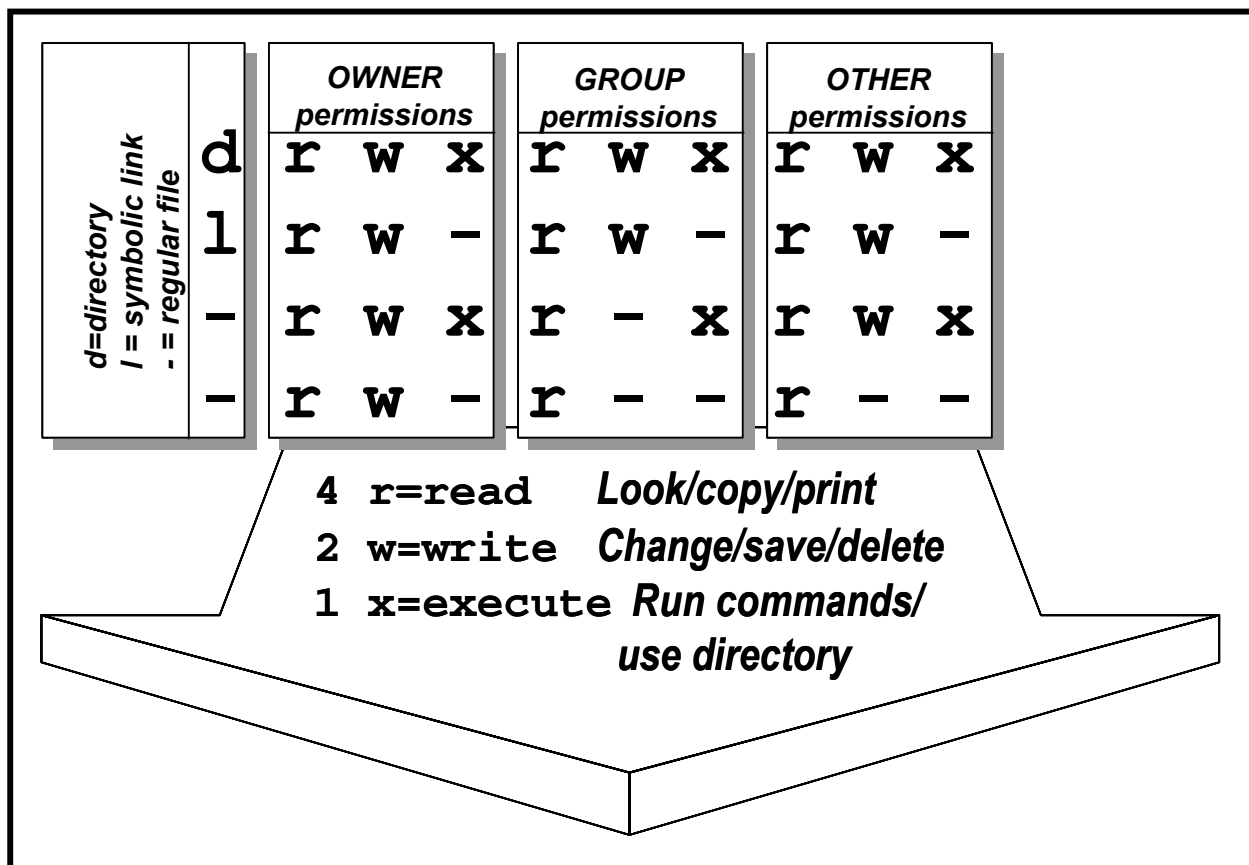
- The first column of output is the file access permission level for the file (see Figure 31 below for a description of file permissions).
  - The next column to the right is the number of links to other files or directories.
  - The third column is the file owner's user ID
  - The fourth column is the group membership of that owner.
  - The fifth column shows file size in bytes.
  - The sixth column displays the date and time of last modification (if the date is more than six months old, the time changes to the year)
  - The last column displays the file name.
- 

## Changing a File/Directory Access Privilege

File and directory access privileges are displayed in the first output column of the **ls -l** command and consist of ten characters, known as **bits**. Each bit refers to a specific permission. The permissions are divided into four groupings shown and briefly described in Figure 31:

In order to perform the procedure, the System Administrator must have obtained the following information about the requester:

- Full path of the file/directory on which access privileges will be changed.
- New access privileges to set on the file/directory. Can be any of:
  - New owner
  - New group
  - New user/owner privileges (read, write and/or execute)
  - New group privileges (read, write and/or execute)
  - New other privileges (read, write and/or execute)



**Figure 31. Access Permissions**

### Changing a File/Directory Access Privilege

- 1 At the UNIX prompt, type **su** then press **Return/Enter**.
- 2 At the **Password** prompt, type **RootPassword** then press **Return/Enter**.
  - Remember that **RootPassword** is case sensitive.
  - You are authenticated as root.
- 3 Type **cd Path** then press **Return/Enter**.
  - The **Path** is the full path up to but not including the file/directory on which access privileges will be changed. For example, if the requester wants access privileges changed on directory **/home/jdoe** type **cd /home** then press **Return/Enter**.



- 4 If there is a **New owner** then type **chown *NewOwner FileOrDirectoryName*** then press **Return/Enter**.
- The ***FileOrDirectoryName*** is the name of the file/directory on which access privileges will be changed minus the path. For example, if the requester wants access privileges changed on directory /home/jdoe type **chown *NewOwner jdoe*** then press **Return/Enter**.
- 5 If there is a **New group** then type **chgrp *NewGroup FileOrDirectoryName*** then press **Return/Enter**.
- The ***FileOrDirectoryName*** is the name of the file/directory on which access privileges will be changed minus the path. For example, if the requester wants access privileges changed on directory /home/jdoe type **chgrp *NewGroup jdoe*** then press **Return/Enter**.
- 6 If there are **New user/owner privileges** type **chmod *u=NewUserPrivileges FileOrDirectoryName*** then press **Return/Enter**.
- The ***FileOrDirectoryName*** is the name of the file/directory on which access privileges will be changed minus the path. For example, if the requester wants access privileges changed on directory /home/jdoe type **chmod *u=NewUserPrivileges jdoe*** then press **Return/Enter**.
  - The ***NewUserPrivileges*** are “r” for read, “w” for write, and “x” for execute. For example, to give the user/owner read, write and execute privileges, type **chmod *u=rwx FileOrDirectoryName*** then press **Return/Enter**.
- 7 If there are **New group privileges** type **chmod *g=NewGroupPrivileges FileOrDirectoryName*** then press **Return/Enter**.
- The ***FileOrDirectoryName*** is the name of the file/directory on which access privileges will be changed minus the path. For example, if the requester wants access privileges changed on directory /home/jdoe type **chmod *g=NewGroupPrivileges jdoe*** then press **Return/Enter**.
  - The ***NewGroupPrivileges*** are “r” for read, “w” for write, and “x” for execute. For example, to give the group read and execute privileges, type **chmod *g=rx FileOrDirectoryName*** then press **Return/Enter**.
- 8 If there are **New other privileges** then type **chmod *o=NewOtherPrivileges FileOrDirectoryName*** then press **Return/Enter**
- The ***FileOrDirectoryName*** is the name of the file/directory on which access privileges will be changed minus the path. For example, if the requester wants access privileges changed on directory /home/jdoe type **chmod *o=NewOtherPrivileges jdoe***, then press **Return/Enter**.

- The *NewOtherPrivileges* are “r” for read, “w” for write, and “x” for execute. For example, to give others read privileges, type **chmod o=r *FileOrDirectoryName*** then press **Return/Enter**.

9 Type **exit** then press **Return/Enter**.

- Root is logged out.
- 

## Moving a User's Home Directory

The Moving a User's Home Directory process begins when the requester submits a request to the Ops Supervisor. The Ops Supervisor approves or denies the request. Once approved, the request is forwarded to the SA who moves the user's home directory. When the changes are complete the SA notifies the requester and Ops Supervisor.

This page intentionally left blank.

# Commercial Off-the-Shelf (COTS) Software Administration

---

The EMD organization provides maintenance for EMD hardware, software, and firmware systems delivered under the EMD contract to the EMD sites.

Commercial off-the-shelf (COTS) software and hardware are maintained in accordance with the current *EMD COTS Deployment Plan*, (335-EMD-series document). The project maintenance philosophy for software is to provide ECS centralized support for developed items and vendor-directed support for COTS software.

## Installation

ECS Project software consists of COTS, custom, and science software.

Software maintenance includes:

- A COTS support contract with the software vendor for license to use, telephone assistance in resolving COTS software problems, obtaining patches and obtaining upgrades.
- Resources, including equipment, software tools and personnel to maintain ECS in accordance with specified functional, performance, and availability requirements.

Services required to produce, deliver, integrate, install, test, validate and document corrections and modifications of existing ECS software and firmware. The maintenance activity includes: software configuration management (CM) including support for change control, configuration status accounting, audit activities, and software quality assurance (QA). Each site is the CM authority over its own resources subject to ESDIS delegation of roles for ECS management.

## Log Files

Log files must be maintained documenting all COTS installations and modifications. These files delineate manufacturer, product, installation date, modification date and all other pertinent configuration data available.

## COTS Configuration

The COTS software upgrades are subject to CCB approval before they may be loaded on any platform. EMD Sustaining Engineering notifies the CCB of the upgrade that has been received. The EMD Property Administrator distributes the COTS software upgrade as directed by the CCB. The site Software Maintenance Engineer, Network Administrator, and the System Administrator are responsible for upgrading the software on the host machine and providing follow-up information to the Configuration Management Administrator (CMA) and the EMD Property Administrator. The site Local Maintenance Coordinator will notify the appropriate

personnel (Release Installation Team, System Administrator, Network Administrator, Software Maintenance Engineer) when the COTS software is received and approved by the CCB for installation.

COTS software patches may be provided by the COTS software vendor in response to a DAAC's call requesting assistance in resolving a COTS software problem. The problem may or may not exist at other locations. When a COTS software patch is received directly from a COTS software vendor (this includes downloading the patch from an on-line source), the DAAC's CCB will be informed via CCR prepared by the requesting Operator, System Administrator, Network Administrator, or site Software Maintenance Engineer. It is the responsibility of the Operator, System Administrator, Network Administrator, or site Software Maintenance Engineer to notify the CCB of the patch's receipt, purpose, and installation status and to comply with the CCB decisions. The Operator, System Administrator, Network Administrator, or site Software Maintenance Engineer installs COTS software patches as directed by the CCB.

In addition to providing patches to resolve problems at a particular site, the software vendor will periodically provide changes to COTS software to improve the product; these changes are issued as part of the software maintenance contract. Upgrades are issued to licensees of the basic software package. Therefore, the COTS software upgrades will be shipped to the EMD Property Administrator, who receives and enters them into inventory.

# Security

---

ECS security architecture must meet the requirements for data integrity, availability, and confidentiality. ECS Security Services meets these requirements by incorporating a variety of mechanisms to establish and verify user accounts, issue and verify passwords, audit user activity, and verify and protect data transfer. To monitor and control access to network services, ECS Security Services uses the public domain tool, TCP Wrappers. Three other public domain COTS products — ANLpasswd, Crack, and SATAN — provide additional password protection for local system and network access. The tool, Tripwire, monitors changes to files and flags any unauthorized changes.

This section defines step-by-step procedures for System Administrators to run the Security Services tools. The procedures assume that the requester's application for a Security process has already been approved by DAAC Management.

## Generating Security Reports

### User Activity Data

A log is created to keep track of unsuccessful attempts to log into the computer. After a person makes five consecutive unsuccessful attempts to log in, all these attempts are recorded in the file `/var/adm/loginlog`. The procedures assume that the file has been created and the operator has logged on as root.

### Reviewing User Activity Data

---

- 1     At the UNIX prompt, type `/usr/bin/logins [-admopstux] [-g group..] [-l login..]` then press **Return/Enter**.
  - 2     Type `logins -x -l username` then press **Return/Enter**.
    - Displays login status for a user.
  - 3     Type `/var/adm/loginlog` then press **Return/Enter**.
    - To enable login Logging, this creates the log file **loginlog**.
  - 4     Type `chmod 600 /var/adm/loginlog` then press **Return/Enter**.
    - This sets read and write permissions for root on the file.
  - 5     Type `chgrep sys /var/adm/loginlog` then press **Return/Enter**.
    - This sets the group to **sys**.
-

## User Audit Trail Information

The **audit\_startup** script is used to initialize the audit subsystem before the audit daemon is started. This script is configurable by the System Administrator, and currently consists of a series of **auditconfig** commands to set the system default policy, and to download the initial events to class mapping. Type the following command to initialize the audit subsystem:

**/etc/security/audit\_startup**

The audit command is the general administrator's interface to the audit trail. The audit daemon may be notified to read the contents of the **audit\_control** file and re-initialize the current audit directory to the first directory listed in the **audit\_control** file or to open a new audit file in the current audit directory specified in the **audit\_control** file as last read by the audit daemon. The audit daemon may also be signaled to close the audit trail and disable auditing. The audit commands are input as shown:

## Audit Commands

**audit -n** then press **Return/Enter**.

- Signals audit daemon to close the current audit file and open a new audit file in the current audit directory.

**audit -s** then press **Return/Enter**.

- Signals audit daemon to read the current audit file. The audit daemon stores the information internally.

**audit -t** then press **Return/Enter**.

- Signals audit daemon to close the current audit file, disable audit and die.

**praudit -sl *filename*** then press **Return/Enter**.

- Displays audit output. The print audit command converts the binary audit records into a variety of formats, depending on the options used with the commands. The format of audit files is included in the file **/usr/include/sys/audit.h**. By default, user IDs (UID) and group IDs (GID) are converted to their ACSII representation.

# Practical Exercises

---

## Introduction

These practical exercises are presented in “day-in-the-life” scenarios relating to system administration activities. They represent real situations that you, as System Administrator, are likely to encounter on a day-to-day basis.

## Equipment and Materials

A functioning ECS computer system.

## System Startup and Shutdown

The EOSDIS system was taken down for maintenance earlier in the day and the maintenance has been completed. You must now bring the system to full operation. Turn on the entire ECS system in the prescribed order.

**-or-**

Startup the following servers:

- SQL Server
- Server 2
- Server 3

## Tape Operations, System Backup and Restore

- 1 You have received an approved request from the Sustaining Engineering Chief to perform an incremental backup of the SQL Server for files created or modified within the past 48 hours.
- 2 Determine how many tapes it will take to back up the required data.
- 3 Prepare the appropriate number of new tapes to accommodate the backup and perform the label and inventory operations on the tapes.
- 4 Perform the incremental backup.
- 5 Inform the Sustaining Engineering Chief that the backup has been performed.



- 6 *xuser* calls you and tells you that she has inadvertently erased the following three files that are critical to her research:
- file1
  - file2
  - file3
- 7 She does not remember exactly when they were last modified. Locate the latest versions of each of the files and perform a file restoration.

## User Administration

- 1 Add a user to the system.

UNIX User Registration Request	
REQUESTER INFORMATION:	
Name:	<u>Erica J. Sonnenshein</u>
Office Phone Number:	<u>(301) 999-5555</u>
E-Mail Address:	<u>esonnens@gsfc.nasa.gov</u>
Office Location:	<u>Bldg. 32</u>
NEW USER INFORMATION:	
Name:	<u>Peter Kovalkaides</u>
Office Phone Number:	<u>(301) 555-1234</u>
Home Phone Number:	<u>(301) 444-4444</u>
Organization:	<u>GSFC DAAC</u>
Group Affiliation(s):	<u>SMC</u>
Role(s)/Job(s)/Justification:	<u>computer operator with database access required</u>
Date of Request:	<u>9/17/97</u>
Date Required:	<u>9/22/97</u>
Supervisor Approval:	_____ Date: _____
Ops Supervisor Approval:	_____ Date: _____

**Figure 32. UNIX User Registration Request Form**

- 2 The user you just added has called you with the news that he has forgotten his password. Describe the procedures you must follow to receive authorization to change the individual's password. Assuming you have received the appropriate authorizations, change the password to gnu-Uzr.
- 3 Change the group affiliations for this user to *new-group affiliation*.
- 4 Peter Kovalkaides sends you an e-mail message informing that the work on his task is complete and requests that you change the access privileges on all files owned by him to READ ONLY for all classes of users to protect the files from changes.
- 5 You have determined that space on the *xserver* is becoming rather scarce. There are a few large files (*insert-file-names-here*) that need to be deleted, and since *xuser* and Peter Kovalkaides are done with their projects, their home directories need to be moved to *insert-new-location-here*. Perform the procedures that will accomplish these tasks assuming you have received the appropriate authorizations. When you are done, inform the affected users of the changes.

## System Maintenance

- 1 The icon on the ECS Desktop for the SQL Server has turned red. Check the system log to find out what the problem is.
- 2 The problem in this exercise requires you to restart the SQL server without affecting any of the other subsystems. Perform this task now.

This page intentionally left blank.

# Slide Presentation

---

## Slide Presentation Description

The following slide presentation represents the slides used by the instructor during the conduct of this lesson.

This page intentionally left blank.